STIC SEARCH REPORT
3/21/06

```
Set      Items   Description
S1       90735    (STORAG? OR WEB OR CACHE?? OR CACHING OR SECUR? OR NETWORK
               OR INTERNET?)(3N)SERVER OR WEBSITE OR WEBPAGE OR ETHERNET? OR
               EXTRANET? OR WWW OR WORLD()WIDE()WEB OR WORLDWIDEWEB OR SUBNE-
               T? OR WAN? ? OR ONLINE
S2      151974    (SECUR? OR ENCOD? OR ENCRYPT? OR CIPHER? OR CYPHER? OR ENC-
               IPHER? OR ENCYPHER? OR LOCK???)(5N)(KEY??? OR CONTAIN??? OR D-
               IGITAL()OBJECT? OR TOKEN? OR DATA OR DATA()FILE? ? OR INFORMA-
               TION?? OR SOFTWARE? OR PROGRAM? OR VPN??) OR PERSONAL()SECUR?-
               ()DEVICE
S3        2058    (REQUEST? OR INQUIR? OR QUERY? OR QUERIES OR ASK??? OR REQ-
               UIS? OR DEMAND??? OR SEEK???)(5N)S2
S4       53779    (DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR T-
               RANSFER? OR TRANSMIT? OR BEAM??? OR PROVID?)(5N)(IDENTIF? OR -
               IDENTIT?)
S5       28727    (DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR T-
               RANSFER? OR TRANSMIT? OR BEAM??? OR PROVID?)(5N)S2
S6       16094    (RECEIV? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR DOWNLOAD? OR -
               PULL???()DOWN?? OR PROCUR??? OR GET? ? OR FETCH??? OR RETRIEV-
               ?)(5N)S2
S7       12076    (CERTIFICAT? OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUT-
               HORIZ? OR AUTHORIS? OR APPROV? OR VERIF? OR KEY??? OR PASSWOR-
               D??)(5N)SERVER??
S8       62520    (DECRYPT? OR DECIPHER? OR DECOD? OR UNLOCK? OR CERTIFICAT?
               OR AUTHENTICAT? OR VERIF?)(3N)(KEY??? OR DEVICE OR MECHANISM??
                OR PASSWORD?? OR CODE? ? OR CODING OR ACCESS?)
S9        1442    (REQUEST? OR INQUIR? OR QUERY? OR QUERIES OR ASK??? OR REQ-
               UIS? OR CHALLENG??? OR DEMAND??? OR SEEK???)(5N)S8
S10       2596    ((DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR -
               TRANSFER? OR TRANSMIT? OR BEAM??? OR PROVID?)(5N)(CERTIFICAT?
               OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUTHORIZ? OR AUTHOR-
               IS? OR VERIF?))(5N)S7
S11       9887    (DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR T-
               RANSFER? OR TRANSMIT? OR BEAM??? OR PROVID?)(5N)S8
S12       7458    (RECEIV? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR DOWNLOAD? OR -
               PULL???()DOWN?? OR PROCUR??? OR GET? ? OR FETCH??? OR RETRIEV-
               ?)(5N)S8
S13     125979   CERTIFICAT? OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUTH-
               ORIZ? OR AUTHORIS? OR APPROV? OR VERIF?
S14        698    (BEFORE? OR PRIOR? OR EARLIER? OR ADVANCE? OR IN()ADVANCE -
               OR AHEAD? OR SUBSEQUEN? OR ALREADY?)(10W)S8
S15      11185   IC=H04K?
S16    1488017   MC=(T01? OR T05? OR W01?)
S17          0   S3 AND S4(10N)S1 AND S5 AND S6 AND S9 AND S10 AND S11 AND -
               S12
S18          0   S3 AND S4 AND S5 AND S6 AND S9 AND S10 AND S11 AND S12
S19         25   S6 AND S12 AND S14
S20         16   S19 AND S15:S16
S21         13   S20 NOT PR>1999
S22         13   IDPAT (sorted in duplicate/non-duplicate order)
S23       1543   S1(10N)S2
S24        974   S23 AND S3:S6
S25        308   S24 AND S7
S26        113   S25 AND S8
S27         79   S26 AND S9:S12
S28          1   S27 AND S14
S29         63   S27 AND S15:S16
S30         49   S29 NOT PR>1999
S31         49   IDPAT (sorted in duplicate/non-duplicate order)
S32         22   S14 AND S15
S33          8   AU=(DUANE W? OR DUANE, W?)
```

```
S34          0   AU=(ROSTIN P? OR ROSTIN, P?)
S35          0   (WILLIAM OR BILL OR BILLY)(2N)DUANE OR (PETER OR PETE)(2N)-
                ROSTIN
S36          8   S33:S35
S37         36   S7 AND S14
S38          1   S37 AND S15
S39         12   S19 NOT S21
S40        224   S14 AND IC=H04L?
S41        198   S40 NOT PR>1999
S42         19   S41 AND S6 AND S12
File 347:JAPIO Nov 1976-2005/Nov(Updated 060302)
         (c) 2006 JPO & JAPIO
File 350:Derwent WPIX 1963-2006/UD,UM &UP=200618
         (c) 2006  Thomson Derwent
```

```
22/3,K/7     (Item 7 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2006  Thomson Derwent. All rts. reserv.

012020893     **Image available**
WPI Acc No: 1998-437803/199837
XRPX Acc No: N98-341073
  Encryption and decryption method especially for paging - encrypting
  message at sender, appending message key then appending senders
  certificate at first server and extracting certificate at second server
Patent Assignee: MOTOROLA INC (MOTI  )
Inventor: SUMNER T E
Number of Countries: 024  Number of Patents: 008
Patent Family:
Patent No      Kind   Date     Applicat No     Kind   Date      Week
WO 9834374      A1  19980806  WO 98US291        A   19980109  199837  B
EP 962072       A1  19991208  EP 98909972       A   19980109  200002
                              WO 98US291        A   19980109
US 6009173      A   19991228  US 97791968       A   19970131  200007
CN 1249096      A   20000329  CN 98802839       A   19980109  200033
KR 2000070624  A   20001125  WO 98US291        A   19980109  200131
                              KR 99706872       A   19990730
CA 2278670      C   20020528  CA 2278670        A   19980109  200249
                              WO 98US291        A   19980109
KR 380125       B   20030416  WO 98US291        A   19980109  200359
                              KR 99706872       A   19990730
CN 1155198      C   20040623  CN 98802839       A   19980109  200612

Priority Applications (No Type Date): US 97791968 A 19970131
Patent Details:
Patent No  Kind Lan Pg   Main IPC     Filing Notes
WO 9834374    A1 E  25 H04L-009/32
   Designated States (National): CA CN IL JP KR RU
   Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC
   NL PT SE
EP 962072     A1 E     H04L-009/32   Based on patent WO 9834374
   Designated States (Regional): DE FR GB
US 6009173    A        H04L-009/32
CN 1249096    A        H04L-009/32
KR 2000070624 A        H04L-009/32   Based on patent WO 9834374
CA 2278670    C  E     H04L-009/32   Based on patent WO 9834374
KR 380125     B        H04L-009/32   Previous Publ. patent KR 2000070624
                                     Based on patent WO 9834374
CN 1155198    C        H04L-009/32

...Abstract (Basic): involves encrypting a message at a sending unit which
    is to be sent to a  receiving  unit using a message  key . The message
    key  encrypted  using a  receiver 's public  key  is appended to the
    message at the sending unit. A sender's certificate is subsequently...

...The sender's certificate is extracted at a second server. The message
    key  is  decrypted  at the  receiving  unit using a  receiver 's
    private  key  to provide a  decrypted  message  key . The message is
    subsequently  decrypted using the  decrypted  message  key .

Manual Codes (EPI/S-X):  W01-A05B ...

... W01-B05A5
```

32/3,K/1   (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO

04131002   **Image available**
MULTIPLEX TRANSMISSION SECRECY SYSTEM FOR TELEVISION SIGNAL

```
PUB. NO.:       05-122702  [JP 5122702  A]
PUBLISHED:      May 18, 1993 (19930518)
INVENTOR(s):    SAITO MASAHIRO
                HAMADA TAKAHIRO
                MATSUMOTO SHUICHI
APPLICANT(s):   KOKUSAI DENSHIN DENWA CO LTD <KDD> [000121] (A Japanese
                Company or Corporation), JP (Japan)
APPL. NO.:      03-307109  [JP 91307109]
FILED:          October 28, 1991 (19911028)
JOURNAL:        Section: E, Section No. 1428, Vol. 17, No. 494, Pg. 86,
                September 07, 1993 (19930907)

INTL CLASS:     H04N-007/167; H04K-001/00 ; H04L-009/32; H04N-007/14
```

ABSTRACT

... from a sender side by a receiver side, comparing a code with a password stored **in advance** and **decoding** a **coding** picture signal for each coincident channel...

32/3,K/2 (Item 2 from file: 347)
DIALOG(R)File 347:JAPIO

03458736 **Image available**
CRYPTOGRAPHIC EQUIPMENT

PUB. NO.: 03-121636 [JP 3121636 A]
PUBLISHED: May 23, 1991 (19910523)
INVENTOR(s): TANAKA TOSHIO
APPLICANT(s): SEIKO EPSON CORP [000236] (A Japanese Company or Corporation)
, JP (Japan)
APPL. NO.: 01-259387 [JP 89259387]
FILED: October 04, 1989 (19891004)
JOURNAL: Section: E, Section No. 1102, Vol. 15, No. 326, Pg. 30,
August 20, 1991 (19910820)

INTL CLASS: **H04K-001/00**

ABSTRACT

... information located in the center, of an input device 4 and an output device 6 **before** and after the cryptographic **coder** 5. A **decoder** 3 consists of a cryptographic decoder 8 based on a neural network learning decoding processing...
...located in the center and of an input device 7 and an output device 9 **before** and after the cryptographic decoder 8. Since the cryptographic **coder** 1 and the **decoder** 3 are constituted with equipments based on the neural network, cryptographic processing not in accordance...

```
32/3,K/22     (Item 19 from file: 350)
DIALOG(R)File 350:Derwent WPIX

(c) 2006  Thomson Derwent. All rts. reserv.

009141407    **Image available**
WPI Acc No: 1992-268845/199232
XRPX Acc No: N92-205613
  Time stamp supplier and digital documents authentication appts. - uses
  sealed digital processor or notary with real-time clock and
  authentication circuit inaccessible from outside
Patent Assignee: BLANDFORD R R (BLAN-I)
Inventor: BLANDFORD R R
Number of Countries: 018  Number of Patents: 002
Patent Family:
Patent No     Kind   Date     Applicat No     Kind    Date     Week
WO 9212485     A1  19920723  WO 91US9270      A   19911210  199232  B
US 5189700     A   19930223  US 89375502      A   19890705  199310
                             US 91637675      A   19910107

Priority Applications (No Type Date): US 91637675 A 19910107; US 89375502 A
  19890705
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
WO 9212485    A1 E  24 G06F-012/14
   Designated States (National): CA JP KR
   Designated States (Regional): AT BE CH DE DK ES FR GB GR IT LU MC NL SE
US 5189700    A      7 H04K-001/00   CIP of application US 89375502


...Abstract (Equivalent): a hash of a text document) and combine the text
    data with the time dat  before  encryption so that the encrypted
    authentication   code  is formed from the combined data...
...International Patent Class (Main):  H04K-001/00
```

```
22/3,K/24     (Item 24 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2006  Thomson Derwent. All rts. reserv.

010619695     **Image available**
WPI Acc No: 1996-116648/199612
Related WPI Acc No: 1995-030540
XRPX Acc No: N96-097599
  Computing system secure access method for shared secret key arrangement -
  providing workstation with password and token, generating transmission
  code with hashing algorithm and verifying validity before transmitting
  session code-encrypted message to workstation for message decryption
Patent Assignee: DIGITAL EQUIP CORP PATENT LAW GROUP (DIGI  )
Inventor: GASSER M; KAUFMAN C W; PEARLMAN R J
Number of Countries: 001  Number of Patents: 001
Patent Family:
Patent No      Kind   Date     Applicat No     Kind   Date      Week
US 5491752      A   19960213  US 9334225        A   19930318  199612  B
                              US 94300576       A   19940902

Priority Applications (No Type Date): US 9334225 A 19930318; US 94300576 A
  19940902
Patent Details:
Patent No  Kind Lan Pg   Main IPC     Filing Notes
US 5491752    A     18 H04K-001/00    Cont of application US 9334225

...Abstract (Basic): a hashing algorithm on data consisting of the token
    and the secret password. The workstation  sends  the transmission code
    to an  authentication   server  for validity  verification .

International Patent Class (Main):  H04K-001/00
```

```
31/3,K/40     (Item 40 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2006  Thomson Derwent. All rts. reserv.

013110767     **Image available**
WPI Acc No: 2000-282638/200024
Related WPI Acc No: 1999-082811; 2001-482278; 2002-235064; 2002-470385
XRPX Acc No: N00-212737
  Secure storage and recovery of core data secrets e.g. passwords,
  cryptographic keys, sensitive personal or financial codes
Patent Assignee: MICROSOFT CORP (MICT  )
Inventor: COOPER A; FIELD S; THOMLINSON M W
Number of Countries: 001  Number of Patents: 001
Patent Family:
Patent No      Kind   Date     Applicat No     Kind   Date      Week
US 6044155      A   20000328  US 97884864      A   19970630  200024  B
                              US 97996634      A   19971223

Priority Applications (No Type Date): US 97996634 A 19971223; US 97884864 A
  19970630
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
US 6044155    A     19 H04K-001/00   CIP of application US 97884864

Abstract (Basic):
...         in a network supervisory computer and returned to and stored in
    a client computer. The encrypted  data  combination is  sent  to the
    network supervisory computer to be  decrypted . The client  key  is
    sent  to the client computer only when the user identification
    corresponds to the currently authenticated user...
...         All encryption, decryption, item integrity checks and user
    authentication  are performed by  storage   server  and associated
    providers , enabling application  programs  to take advantage of
    advanced  security  features without adding complexity to application
    programs. Default storage  1provider  implements multilevel  key
    encryption  scheme to minimize amount of encryption that has to be
    re-done when user changes...
International Patent Class (Main):  H04K-001/00
Manual Codes (EPI/S-X):  T01-J05A1 ...

... T01-J12C ...

... T05-L02 ...

... T05-L03C5 ...

... W01-A05B
```

Your Appl.

Your assignee

```
36/3,K/4     (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2006  Thomson Derwent. All rts. reserv.

013896614     **Image available**
WPI Acc No: 2001-380827/200140
XRPX Acc No: N01-279240
  Secure information providing method for cryptography application,
  involves providing decryption information for personal security device in
  response to authentication information
Patent Assignee: RSA SECURITY INC (RSAS-N)
Inventor:  DUANE W ; ROESTIN P
Number of Countries: 094  Number of Patents: 003
Patent Family:
Patent No      Kind   Date     Applicat No      Kind   Date      Week
WO 200106699    A2   20010125  WO 2000US19656   A    20000719  200140  B
AU 200062226    A    20010205  AU 200062226     A    20000719  200140
EP 1201070      A2   20020502  EP 2000948778    A    20000719  200236
                               WO 2000US19656   A    20000719

Priority Applications (No Type Date): US 99356600 A 19990719
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
WO 200106699  A2 E  36 H04L-009/00
   Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA
   CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP
   KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT
   RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
   Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR
   IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW
AU 200062226  A        H04L-009/00   Based on patent WO 200106699
EP 1201070    A2 E     H04L-029/06   Based on patent WO 200106699
   Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT
   LI LT LU LV MC MK NL PT RO SE SI

Inventor:  DUANE W ...
```

39/3,K/7 (Item 7 from file: 347)
DIALOG(R)File 347:JAPIO

05737679 **Image available**
KEY CHANGING METHOD IN OPEN KEY CIPHER SYSTEM

PUB. NO.: 10-020779 [JP 10020779 A]
PUBLISHED: January 23, 1998 (19980123)
INVENTOR(s): KOBORI MASAHIRO
SHIOMI YOSHIHIRO
APPLICANT(s): HITACHI INF SYST LTD [490611] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 08-177673 [JP 96177673]
FILED: July 08, 1996 (19960708)

ABSTRACT

...and electronic signed data smoothly with a past key so as to be able to **obtain** transmitter authorization after the **key** change of an open **key** **cipher** system...

... to which data was actually sent before the change of the key, and the data **before** the change of the secret key and open **key** is **decoded** on the transmitted side to confirm a signature. In decoding processing on the receiving side...
...key or not is judged, and in the negative case, the old secret key is **retrieved** from the secret **key** table 201 to **decode** the data with the **retrieved** old secret key.

39/3,K/8 (Item 8 from file: 347)
DIALOG(R)File 347:JAPIO

05499987 **Image available**
METHOD AND SYSTEM FOR INFORMATION DISTRIBUTION

PUB. NO.: 09-114787 [JP 9114787 A]
PUBLISHED: May 02, 1997 (19970502)
INVENTOR(s): AKASHI OSAMU
MORIYASU KENJI
TERAUCHI ATSUSHI
APPLICANT(s): NIPPON TELEGR & TELEPH CORP <NTT> [000422] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 07-274324 [JP 95274324]
FILED: October 23, 1995 (19951023)

ABSTRACT

... system capable of performing the authentication and settlement of accounts as necessary and referring to **information** by decoding the **information** being a **ciphered** article by using the **decoding key obtained** from a key center and utilizing the information...

...SOLUTION: An information center 2 ciphers the provided **information** and imparts **information** identification ID to the **ciphered information** article. A **key** center 3 **receives** the information identification ID and a decoding key from the information center 2, controls them...

...information article in exchange for the reception to a using terminal. A using terminal 4 **obtains** identifier and the **ciphered information** article and confirms that the information is not fraudulently altered by authenticator. When the decision...

... identifier part or the reception is performed, the charge for the information article is paid **before** the decoding of information. As for the **key** for a **decoding** in exchange for the payment, the **decoded key** is **received** from the key center 3 by keeping the key secret from a third party by...

39/3,K/9   (Item 9 from file: 347)
DIALOG(R)File 347:JAPIO

02716234   **Image available**
KEY DISTRIBUTION SYSTEM FOR MULTIPLE ADDRESS COMMUNICATION

PUB. NO.:	01-013834 [JP 1013834 A]
PUBLISHED:	January 18, 1989 (19890118)
INVENTOR(s):	OKAMOTO EIJI
APPLICANT(s):	NEC CORP [000423] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.:	62-171539 [JP 87171539]
FILED:	July 08, 1987 (19870708)
JOURNAL:	Section: E, Section No. 753, Vol. 13, No. 192, Pg. 123, May 09, 1989 (19890509)

ABSTRACT

...list of cryptographic keys for each terminal at a center by allowing the center to **receive** **key** distribution **data** generated at terminals and to **encipher** the **key** selected optionally based on the said data to send the result to terminals...

...the WK and sends the result EK to the user 1. When the EK is **received** , the user 1 uses the **key** calculated **already** to **decode** the EK thereby **obtaining** the WK. Moreover, other users than the user 1 obtain similarly the WK.

```
Set      Items   Description
S1      447672    (STORAG? OR WEB OR CACHE?? OR CACHING OR SECUR? OR NETWORK
                OR INTERNET?)(3N)SERVER OR WEBSITE OR WEBPAGE OR ETHERNET? OR
                EXTRANET? OR WWW OR WORLD()WIDE()WEB OR WORLDWIDEWEB OR SUBNE-
                T? OR WAN? ? OR ONLINE OR INTERNET? OR NETWORK?
S2      161745    (SECUR? OR ENCOD? OR ENCRYPT? OR CIPHER? OR CYPHER? OR ENC-
                IPHER? OR ENCYPHER? OR LOCK???)(5N)(KEY??? OR CONTAIN??? OR D-
                IGITAL()OBJECT? OR TOKEN? OR DATA OR DATA()FILE? ? OR INFORMA-
                TION?? OR SOFTWARE? OR PROGRAM? OR VPN??) OR PERSONAL()SECUR?-
                ()DEVICE
S3        6057    (REQUEST? OR INQUIR? OR QUERY? OR QUERIES OR ASK??? OR REQ-
                UIS? OR DEMAND??? OR SEEK???)(5N)S2
S4       74996    (DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR T-
                RANSFER? OR TRANSMIT? OR BEAM??? OR PROVID?)(5N)(IDENTIF? OR -
                IDENTIT?)
S5       42908    (DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR T-
                RANSFER? OR TRANSMIT? OR BEAM??? OR PROVID?)(5N)S2
S6       26362    (RECEIV? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR DOWNLOAD? OR -
                PULL???()DOWN?? OR PROCUR??? OR GET? ? OR FETCH??? OR RETRIEV-
                ?)(5N)S2
S7       91622    (CERTIFICAT? OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUT-
                HORIZ? OR AUTHORIS? OR APPROV? OR VERIF? OR KEY??? OR PASSWOR-
                D??)(5N)SERVER?? OR SERVER?
S8       64601    (DECRYPT? OR DECIPHER? OR DECOD? OR UNLOCK? OR CERTIFICAT?
                OR AUTHENTICAT? OR VERIF?)(3N)(KEY??? OR DEVICE OR MECHANISM??
                 OR PASSWORD?? OR CODE? ? OR CODING OR ACCESS?)
S9        4382    (REQUEST? OR INQUIR? OR QUERY? OR QUERIES OR ASK??? OR REQ-
                UIS? OR CHALLENG??? OR DEMAND??? OR SEEK???)(5N)S8
S10       4804    ((DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR -
                TRANSFER? OR TRANSMIT? OR BEAM??? OR PROVID?)(5N)(CERTIFICAT?
                OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUTHORIZ? OR AUTHOR-
                IS? OR VERIF?))(5N)S7
S11      14837    (DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR T-
                RANSFER? OR TRANSMIT? OR BEAM??? OR PROVID?)(5N)S8
S12      13341    (RECEIV? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR DOWNLOAD? OR -
                PULL???()DOWN?? OR PROCUR??? OR GET? ? OR FETCH??? OR RETRIEV-
                ?)(5N)S8
S13     278526    CERTIFICAT? OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUTH-
                ORIZ? OR AUTHORIS? OR APPROV? OR VERIF?
S14       4463    (BEFORE? OR PRIOR? OR EARLIER? OR ADVANCE? OR IN()ADVANCE -
                OR AHEAD? OR SUBSEQUEN? OR ALREADY?)(10W)S8
S15     230469    IC=(H04L? OR H04K? OR G06F?)
S16      15286    S1(10N)S2
S17       2602    S16 AND S3
S18       1392    S17 AND S4
S19        518    S18 AND S5(10N)S6
S20        234    S19 AND S7(10N)S8
S21         20    S20 AND S9(10N)S10(10N)S11
S22         16    S21 AND S12
S23         11    S22 AND S14
S24          2    S23 NOT AD=2000:2006
S25       2350    S14 AND S15
S26        712    S25 NOT AD=2000:2006
S27         23    S26 AND S4(20N)S12
S28         23    IDPAT (sorted in duplicate/non-duplicate order)
S29         87    S16 AND S6(20N)S12(20N)S14
S30         67    S29 AND S15
S31         16    S30 NOT AD=2000:2006
S32         41    S21:S24 OR S28
S33          9    S31 NOT S32
S34        760    S1:S2 AND ELECTRON?(3N)(WALLET? OR BRIEFCASE? OR BILLFOLD?
```

FT Pat files

```
             OR ENCASE?)
S35        427   S34 AND S15
S36        112   S35 NOT AD=2000:2006
S37    1554084   BEFORE? OR PRIOR? OR EARLIER? OR ADVANCE? OR IN()ADVANCE OR
              AHEAD? OR SUBSEQUEN? OR ALREADY?
S38         47   S36 AND S37(10W)(S13 AND S8)
S39         98   S30:S33
S40         38   S38 NOT S39
S41         10   AU=(DUANE W? OR DUANE, W?)
S42          6   AU=(ROSTIN P? OR ROSTIN, P?)
S43         18   (WILLIAM OR BILL OR BILLY)(2N)DUANE OR (PETER OR PETE)(2N)-
             ROSTIN
S44         22   S41:S43
S45          6   S41 AND S42
S46          8   S44 AND S15
S47          6   S45 AND S15
S48          8   S46:S47
S49          0   S48 NOT AD=2000:2006
S50         46   S48 OR S40
S51         46   IDPAT (sorted in duplicate/non-duplicate order)
File 348:EUROPEAN PATENTS 1978-2006/ 200611
         (c) 2006 European Patent Office
File 349:PCT FULLTEXT 1979-2006/UB=20060316,UT=20060309
         (c) 2006 WIPO/Univentio
```

```
24/3,K/1     (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2006 European Patent Office. All rts. reserv.

01796015
Mobile electronic commerce system
Mobiles elektronisches Handelssystem
Systeme de commerce electronique mobile
PATENT ASSIGNEE:
  MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD, (216884), 1006, Oaza-Kadoma,
    Kadoma-shi, Osaka 571-0000, (JP), (Applicant designated States: all)
INVENTOR:
  Takayama, Hisashi, 5-6-12-104 Matsubara, Setagaya-ku Tokyo 156-0043, (JP)
LEGAL REPRESENTATIVE:
  Grunecker, Kinkeldey,  Stockmair & Schwanhausser Anwaltssozietat (100721)
    , Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date):  EP 1467300  A1  041013 (Basic)
APPLICATION (CC, No, Date):   EP 2004015278 980813;
PRIORITY (CC, No, Date): JP 97230564 970813
DESIGNATED STATES: DE; FR; GB
RELATED PARENT NUMBER(S) - PN (AN):
  EP 950968  (EP 98937807)
INTERNATIONAL PATENT CLASS (V7): G06F-017/60; H04Q-007/32; G07F-007/08
ABSTRACT WORD COUNT: 150
NOTE:
  Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text  Language   Update    Word Count
      CLAIMS A  (English)  200442     17631
      SPEC A    (English)  200442    160348
Total word count - document A        177979
Total word count - document B             0
Total word count - documents A + B  177979

...SPECIFICATION process is terminated.
    Then, following the subtraction of its commission, the ticket retail
  store 13820  1transmits  a record of the receipts for the sale of the
  ticket to the ticket issuer 13821, which, in turn, subtracts its
  commission from the record of receipts and  transmits  the result to the
  promotor of the event for which the ticket was sold (13834...

...vending system, when a concert, for example, is canceled after a ticket
  is issued, to  receive  a refund the consumer must return to the ticket
  retail store, an additional inconvenient requirement...
...a supply side, a product or a service, or a required permission, service
  means is  provided  for connecting the electronic wallet and the supply
  side via the communication means. The service...

...electronic telephone card can be purchased via the service means, and
  for use can be  downloaded  into the electronic wallet. Usability can
  therefore be improved.
    According to the invention cited in...

...means for communicating with the electronic wallet;
     radio communication means for communicating with the service
  providing  means;
     product  identification  means for identifying a product type;
     input means for entering a numerical value and for...payment card that
```

is issued by the payment card issuing means, and for use, can **download** it to the electronic wallet. As a result, usability is improved.
According to the invention...

...According to the invention cited in claim 51, the electronic telephone card settlement means, upon **receiving** the telephone micro-check message, generates and then transmits, to the electronic wallet, a receipt message acknowledging that the telephone micro-check message has been **received** .
Thus, the owner of the electronic wallet can confirm the contents of a wireless communication...

...be efficiently examined.
According to the invention cited in claim 54, the electronic wallet, upon **receiving** a command message from the electronic ticket examination means, changes the electronic ticket to a post-examined state, and generates and then **transmits** , to the electronic ticket examination means, a ticket examination response message that describes the contents ...

...wallet; the second electronic wallet transmits, to the service providing means, the payment card transfer **certificate** message that is received; the service **providing** means performs an examination to establish the validity of the payment card **transfer** certificate message that is **received** , and **transmits** , to the second electronic wallet, the electronic payment card that is described in the payment...

...is improved.
According to the invention cited in claim 57, the second electronic wallet, upon **receiving** the payment card **transfer** **certificate** message, generates a payment card receipt message confirming that the payment card transfer certificate message...

...certificate message via wireless communication means to the second electronic wallet; the second electronic wallet **transmits** , to the service **providing** means, the telephone card **transfer** certificate message that is received; the service providing means performs an examination to establish the...

...electronic wallet stores, in the second storage means thereof, the electronic telephone card that is **received** .
Therefore, the electronic telephone card can be transferred to another person, and usability is improved...

...transfer certificate message, generates a telephone card receipt message confirming that the telephone card transfer **certificate** message has been **received** , and transmits the telephone card receipt message via the wireless communication means to the first...

...an electronic telephone card or an electronic ticket, of a type described using the first **identification** information, that is to be installed. The second identification information is information generated at random...

...message for the modification of the contents of the electronic ticket; the electronic wallet, upon **receiving** the modification notification message, generates and then transmits, to the service providing means, a reaction...

...message for the modification of the contents of the electronic ticket;

the electronic wallet, upon **receiving** the modification notification message, generates and then transmits, to the service providing means, a reaction...

...electronic payment card to the usable state.
Since an electronic payment card must be registered **before** it can be used, if a sleeping electronic payment card that is not registered for... wallet, an electronic ticket that is stored in the second storage means; and the service **providing** means, upon **receiving** the ticket registration request message, registers the electronic ticket for use in the service director...

...public key, which is paired with the accounting device authentication private key, and a card **authentication** private key, which is paired with the card **authentication** public **key** .
Therefore, the electronic wallet and the electronic payment card settlement means can mutually perform the...

...performed by the electronic telephone card. The digital signature of the owner of the service **providing** means is **provided** for the presented card information.
As a result, the settlement of a communication fee by...

...private key and a card authentication public key. The telephone card program includes an accounting **device** **authentication** public **key** , which is paired with the accounting **device** **authentication** private **key** , and a card **authentication** private **key** , which is paired with the card authentication public key.
Therefore, the electronic wallet and the...

...by individual telephone card issuers.
According to the invention cited in claim 93, the template **program** for the electronic telephone card includes:
a transaction module program for the electronic telephone card...

...when issued; and
a ticket certificate indicating that the electronic ticket is authentic. The ticket **program** includes:
electronic ticket state management **information** ; and
ticket **program** **data** for specifying an operation to be performed by the electronic ticket. The digital signature of...

...card can be performed safely.
According to the invention cited in claim 95, the ticket **program** includes a ticket signature private **key** that is employed for a digital signature provided for the electronic ticket. The ticket certificate...

...a message generated by the electronic ticket, and the validity of the message can be **verified** .
According to the invention cited in claim 96, an examination **program** module for the electronic ticket includes two cryptographic **keys** , a gate authentication private key and a ticket authentication public key. The ticket card program...

...key, and a ticket authentication private key, which is paired with the ticket authentication public **key** .
Therefore, the electronic wallet and the electronic ticket examination means can mutually perform the authentication...
...are exchanged by the electronic wallet and the electronic ticket examination means;

a display module **program** for specifying the manner in which the electronic ticket is to be displayed; and
representative...

...card issuance request message or the electronic payment card installation request message includes template program **identification** information for designating, in the order to be used for the generation of an electronic...

...one of a plurality of template programs that are stored in the payment card issuer **information** storage means.
Therefore, the payment card issuing means can designate a template program to be...

...payment cards.
According to the invention cited in claim 102, the electronic payment card issuance **request** message or the electronic payment card installation **request** message includes representative component **information** describing the representative component **information** to be used for an electronic payment card that is to be generated.
Therefore, selected...

...electronic payment card stored in the second storage means for the electronic wallet; the service **providing** means, upon receiving the payment card registration request message, newly generates, for the electronic payment...

...by the input means of the electronic wallet;
presented card information and a registered card **certificate** for the electronic payment card; and
state management information to which a digital signature has...

...the electronic payment card to the second electronic wallet.
Therefore, the side that is to **transfer** the electronic payment card and the side that is to receive the electronic payment card...

...second electronic wallet is provided for the payment card transfer offer message; the payment card **transfer** certificate message includes **identification** information for the public **key** **certificate** of the owner of the first electronic wallet and identification information for the public key...
...card issuance request message or the electronic telephone card installation request message includes template program **identification** information for designating, following the order that is to be used for the generation of...

...stored in the second storage means for the electronic wallet; the service providing means, upon **receiving** the telephone card registration request message, newly generates, for the electronic telephone card, a card...

...According to the invention cited in claim 121 the micro-check call request message includes:
identification information for the side that is designated by the input means of the electronic wallet...

...check message includes:
a payment amount;
a amount remaining stored on the electronic telephone card;
identification information for the electronic telephone card

settlement means; and
identification information for the owner of...provisions of the transfer.

According to the invention cited in claim 127, the telephone card **transfer** offer message includes:
presented card information and a card certificate or a registered card certificate...

...first electronic wallet is provided for the telephone card transfer offer message; the telephone card **transfer** offer response message includes a public key certificate for the owner of the second electronic ...

...registered ticket certificate that are stored by replacing them with those that have been newly **received** , and changes the state management **information** for the electronic ticket to a usable state.
Since for use the signature key for...

...in the second storage means for the electronic ticket examination means, and generates and then **transmits** , to the electronic wallet, an examination certificate message certifying that the electronic ticket has been...

...management information for the electronic ticket;
identification information for the electronic ticket examination means; and
identification information for the owner of the electronic ticket examination means. Further, a digital signature is...

...the ticket examination response message includes identification information for the electronic ticket examination means and **identification** information for the owner of the electronic ticket examination means. Further, the digital signature prepared...

...According to the invention cited in claim 140, a first electronic wallet generates a ticket **transfer** offer message offering to **transfer** , to a second electronic wallet, an electronic ticket that is stored in the second storage...

...means to the first electronic wallet; and the first electronic wallet, upon receiving the ticket **transfer** offer response message, generates and then **transmits** , to the second electronic wallet, a ticket **transfer** certificate message confirming the **transfer** of the electronic ticket to the second electronic wallet. Therefore, the side that is to...

...of the second electronic wallet is provided for the ticket transfer offer message; the ticket **transfer** certificate message includes **identification** information for the public key certificate for the owner of the first electronic wallet and identification information for the public **key certificate** for the owner of the second electronic wallet; and a digital signature using a ticket...

...claims 41 to 146 is recorded in a form readable by a computer. Thus, the **program** can be distributed in a portable form.
According to the invention cited in claim 158...to the embodiment of the present invention;
Fig. 92B is a specific diagram showing the **data** structure for an electronic ticket issuing in the ticket purchase processing according to the embodiment...

...Fig. 95A is a specific diagram showing the data structure of a receipt that is **transmitted** , in the ticket purchase processing, from the ticket issuing system to the service system according...

...to the embodiment of the present invention;
Fig. 97A is a specific diagram showing the **data** structure of an electronic payment card issuing commission for the payment card purchase processing according...
...to the embodiment of the present invention;
Fig. 132B is a specific diagram showing the **data** structure of a refund clearing receipt according to the embodiment of the present invention;
Fig...to the embodiment of the present invention;
Fig. 138A is a specific diagram showing the **data** structure of a receipt that is transmitted, in the real credit settlement processing, from the...

...card issuing system
109: telephone card issuing system
110: service system
111: digital public line **network**
112, 113, 114, 201: base station
115: telephone terminal
207: installation card
300, 400, 501...

...switch
306, 606: end switch
307, 506, 607; function switch
308, 403, 507, 608: number **key** switch
309, 402, 509, 611: power switch
310, 609: microphone
311, 508, 612: execution switch...

...data processor
803: modulator/demodulator
804: base station controller
900: service server
901: server director **information** server
902: user **information** server
903: merchant **information** server
904: transaction processor information server
905: ticket issuer information server
906: payment card issuer...

...ATM-LAN switch
911, 1005, 1105, 1205, 1305: ATM switch
1000: transaction server
1001: subscriber **information** server
1002: member store **information** server
1003: transaction **information** server
1100: ticket issuing server
1101, 1201, 1301: customer information server
1102: ticket issuing information...

...1203: payment card information server
1300: telephone card issuing server
1302: telephone card issuing information **server**
1303: telephone card information server
1400: electronic payment card installation card

1401: electronic telephone card...

...base station 114, which connects the automatic vending machine 104 to the digital public line **network** 111; and a destination telephone terminal 115, which is connected to the digital public line...

...a digital communication line for connecting the base station 114 to the digital public line **network** 111; 129, a telephone communication line for connecting the telephone terminal 115 to the digital public line **network** 111; 130, a digital communication line for connecting the digital public line network 111 to...mode to the digital telephone mode, and then enters a phone number using the number **key** switches 507. Through the above operation, the operator (merchant) can place a call to a...

...604 to set the operating mode to the merchant mode. The operator reads the bar **code** for a product using the bar **code** reader 610, and depresses the total switch in the number key switches 608 to calculate...

...switching for a digital wireless telephone network, and the switching for the digital wireless telephone **network** and the digital public line **network** 111; 802, a **data** processor for **encoding** and decoding sound and **data** ; 803, a modulator/demodulator for performing a multiplexing process and a modulation/demodulation process; and...

...108, and the telephone card issuing system 109. The service system 100 comprises: a service **server** 900, for controlling data communication; a service director information server 901, for managing attribute information...

...attribute information and the data stored in the mobile user terminal 100; a merchant information **server** 903, for managing the attribute information for the merchant and the communication provider and for... 908, with which the service provider manages the operation of the service system 110. The **servers** 900 to 907 and the management system 908 are constituted by one or more computers...

...processor information server 904, the ticket issuer information server 905, the payment card issuer information **server** 906, and the telephone card issuer information **server** 907 are respectively connected to an ATM-LAN switch 909 by ATM-LAN cables 914...

...909, the service director information server 901, the user information server 902, the merchant information **server** 903, the transaction processor information **server** 904, the ticket issuer information **server** 905, the payment card issuer information **server** 906, and the telephone card issuer information **server** 907.

The ATM-LAN switch 909 is connected to an ATM switch 911 by an...

...more computers.

The transaction server 1000, the subscriber information server 1001, the member store information **server** 1002, and the transaction information **server** 1003 are respectively connected to an ATM-LAN switch 1004 by ATM-LAN cables 1008...

...connection with the service system 110 is connected to the ATM switch 1005. The transaction **server** communicates with the service system 110 via the ATM-LAN switch 1004 and the ATM...

...between the transaction server 1000 and the bank on-line system, and between the transaction **server** 1000 and the transaction processing system of another transaction processor, the ATM switch 1005 converts...

...1304 by ATM-LAN cables 1308, 1309, 1310 and 1311. The telephone card issuing server **accesses** , via the ATM-LAN switch 1304, the customer information **server** 1301, the telephone card information **server** 1302, or the telephone card information **server** 1303.

The ATM-LAN switch 1304 is connected to an ATM switch 1305 by an...

...electronic payment card that is to be installed. In order to prevent the leakage of **identification** information during **distribution** , a coating is applied to the portion whereon the installation card number 1407 and the...

...ticket to be installed; and a 32-digit installation number 1420 that corresponds to an **identification** number for the same type of electronic ticket. The coating is applied to the portion...ticket issuing system, the ticket issuing server 1100 updates the data in the customer information **server** 1101, in the ticket issuing information **server** 1102, and in the ticket information **server** 1103. The ticket issuing **server** 1100 generates ticket data for the ordered ticket, and transmits, to the service providing system...

...information server 1001, in the member store information server 1002 and in the transaction information **server** 1003, performs a clearing process for the credit card, and transmits to the service providing...

...of the received ticket registration request 6501 with the user information in the user information **server** 902. The service **server** 900 updates the management information that is stored in the service director information server 901...which the amount charged is given as the face value. The micro-check 6807 is **transmitted** to the merchant terminal via infrared communication.

The merchant terminal examines the contents of the...

...102 or 103 or the automatic vending machine 104 generates and transmits, to the service **providing** system, **upload** data 5704, which is a message in which is included the data that is to be **uploaded** to the service **providing** system. At this time, the upload data 5704 includes information for a new micro-check...

...examines the micro-check to determine whether it is valid. Then, the service server 900 **transmits** , to the merchant terminal 102 or 103 or the automatic vending machine 104, an update...

...or 103, in accordance with the contract agreed to by the merchant and the service **providing** system, the payment card reference results may be transmitted to the...transfer operation 7500). Then, via infrared communication, the mobile user terminal belonging to user A **transmits** , to the mobile user terminal belonging to user B, a payment card transfer offer 7501...

...received as a gift. The telephone card setup process is a process whereby the service **provider** determines the process to be employed for the electronic telephone card at the electronic telephone...

...after the electronic telephone card is purchased, or while an electronic telephone card that has **not** yet been registered is displayed ("unregistered" is displayed as the state of the telephone card... terminal, an authorization response 8411, which is a response message for the authorization request.

Upon **receiving** the authorization response 8411 from the service providing system 110, the merchant terminal displays, on...

...that the settlement process has been completed is transmitted to the service providing system.

Upon **receiving** the clearing completion notification 8417, the service providing system generates a clearing completion notification 8418...

...terminal 100 displays, on the LCD, the contents of the receipt 8421 that has been **received** , and notifies the user of the completion of the settlement process (display the receipt: 8422...

...transmitted and decodes data that is received; an infrared communication module 1507, which transmits and **receives** infrared rays during infrared communication; a **key** operator 1509, which detects the manipulation by the user of the mode switch 304, the...

...the audio codec 1512 and the channel codec.

The cryptographic processor 1505 includes a secret **key** encryption and decryption function and a public **key** **encryption** and decryption function. The cryptographic processor 1505 employs a cryptography method determined by the CPU 1500 and the **keys** to **encrypt** or decrypt **data** set by the CPU 1500. The encryption and decryption functions of the cryptographic processor 1505...

...signature process or a closing process for a message, and to decrypt a closed and **encrypted** message or to verify a digital signature accompanying a message. A detailed explanation will be...

...data that is received under the control of the CPU 1500. In this case, the **encoding** is a process for generating **data** to be transmitted that includes communication control information and error correction information, and the decoding is a process for performing error correction for the **received** data and for removing extra communication control information in order to **obtain** the data that a sender was originally to transmit. The data codec 1506 has a function for **encoding** or decoding **data** during **data** communication performed using a digital wireless telephone, and a function for encoding or decoding data...

...to perform a digital signature process and a closing process for a message, employs the **data** codec 1506 to **encode** the **obtained** message to **provide** a data communication form for a digital wireless telephone, and transmits the resultant message via...

...message from the channel codec 1513 through the control logic unit 1508, employs the data **codec** 1506 to **decode** the **received** message, and permits the cryptographic processor 1505 to decrypt the closed and encrypted message and...

...provide a digital signature for the message and to close the message, and employs the **data** codec 1506 to **encode** the **obtained** message to **provide** a data form suitable for infrared communication. Then, the resultant message is transmitted to the...

...the CPU 1500 reads that message from the infrared communication module 1507, employs the data **codec** 1506 to **decode** the **received** message, and permits the cryptographic processor 1505 to decrypt the closed and encrypted message and...

...is transmitted to the audio processor 1511, which amplifies the signal 1543 and drives the **receiver** 302 to produce sounds. The **encoded** digital audio **data** are **transmitted** as a digital audio signal 1546 to the channel codec 1513, which converts the data...

...be transmitted across the radio channel.

In addition, the audio codec 1512 includes an audio **data** **encryption** **key** register (CRYPT) 1613 in which is stored an **encryption** **key** for the secret **key** cryptography method that is employed for encryption and decryption of audio **data** . When the audio **data** **encryption** **key** is set to the audio **data** **encryption** **key** register (CRYPT) 1613 by the CPU 1500, the audio codec 1512 encodes the analog audio signal 1542 to provide digital audio **data** , and at the same time **encrypts** the digital audio **data** , or decodes the digital audio data to provide an analog audio signal 1543 while simultaneously decrypting the audio data.

Two types of data to be transmitted are **received** by the channel **codec** 1513: one type is digital audio data originating at the audio codec 1512 as a...9 for the number key switch 208. Bit 10 and bit 11 correspond to number **key** switches "*" and "#" and bits 12 to 15 corresponds to function switches F1 to F4. Bits...

...1802, a personal information address 1803, a portrait image data address 1804, a user public **key** **certificate** address 1805, a user preference address 1806, a telephony information address 1807, a credit card...

...is stored. And the access time 1839 is the time at which the user last **accessed** the electronic telephone card.

A local address indicating an address in the object data area...

...an electronic ticket, and a ticket signature private key 1910 and a ticket signature public **key** 1925 (1936) are provided as a private key and a corresponding public key. Another key...

...CLAIMS means for communicating with said electronic wallet;

radio communication means for communicating with said service **providing** means;

product **identification** means for identifying a product type;

input means for entering a numerical value and for...electronic wallet is provided for said payment card transfer offer message; wherein said payment card **transfer** certificate message includes **identification** information for said public key certificate of said owner of said first electronic wallet and...

...electronic wallet is provided for said telephone card transfer offer message; wherein said telephone card **transfer** certificate message includes **identification** information for said public key certificate for said owner of said first electronic wallet and...

...said second electronic wallet is provided for said ticket transfer offer message; wherein said ticket **transfer** certificate message includes **identification** information for said public key certificate for said owner of said first electronic wallet and...generating first identification information for identifying a transaction conducted with said supply side, and for **transmitting** said first **identification** information to said supply side; wherein said supply side includes means for generating second identification information for identifying a transaction conducted with said electronic wallet, and for **transmitting** said second **identification** information to said electronic wallet; wherein said electronic wallet includes means for generating said electronic...

...identifying an electronic payment card transfer process performed with said second electronic wallet, and for **transmitting** said first **identification** information to said second electronic wallet; wherein said second electronic wallet includes means for generating...

...identifying an electronic payment card transfer process performed with said first electronic wallet, and for **transmitting** said second **identification** information to said first electronic wallet; wherein said first electronic wallet includes means for generating...

...identifying an electronic telephone card transfer process performed with said second electronic wallet, and for **transmitting** said first **identification** information to said second electronic wallet; wherein said second electronic wallet includes means for generating...

...identifying an electronic telephone card transfer process performed with said first electronic wallet, and for **transmitting** said second **identification** information to said first electronic wallet; wherein

said first electronic wallet includes means for generating...

...for identifying an electronic ticket transfer process performed with said second electronic wallet, and for **transmitting** said first **identification** information to said second electronic wallet; wherein said second electronic wallet includes means for generating...

...for identifying an electronic ticket transfer process performed with said first electronic wallet, and for **transmitting** said second **identification** information to said first electronic wallet; wherein said first electronic wallet includes means for generating...

...for identifying a negotiable card transfer process performed with said second electronic wallet, and for **transmitting** said first **identification** information to said second electronic wallet; wherein said second electronic wallet includes means for generating...

...for identifying a negotiable card transfer process performed with said first electronic wallet, and for **transmitting** said second **identification** information to said first electronic wallet; wherein said first electronic wallet includes means for generating...

```
28/3,K/12     (Item 12 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2006 European Patent Office. All rts. reserv.

01097041
DATA  TRANSMITTING/RECEIVING  METHOD, DATA TRANSMITTER, DATA RECEIVER, DATA
    TRANSMITTING/RECEIVING  SYSTEM,  AV  CONTENT  TRANSMITTING  METHOD,  AV
    CONTENT  RECEIVING METHOD, AV CONTENT TRANSMITTER, AV CONTENT RECEIVER,
    AND PROGRAM RECORDING MEDIUM
VERFAHREN  ZUM  SENDEN/EMPFANGEN  VON  DATEN,  DATENSENDER, DATENEMPFANGER,
    EINRICHTUNG  ZUM SENDEN/EMPFANGEN VON DATEN, VERFAHREN ZUM SENDEN EINES
    AUDIOVISUELLEN  INHALTS,  VERFAHREN  ZUM EMPFANGEN EINES AUDIOVISUELLEN
    INHALTS,  SENDER  UND  EMPFANGER  EINES  AUDIOVISUELLEN  INHALTS,  UND
    PROGRAMMAUFZEICHUNGSMEDIUM
PROCEDE  D'EMISSION/RECEPTION DE DONNEES, EMETTEUR DE DONNEES, RECEPTEUR DE
    DONNEES, SYSTEME D'EMISSION/RECEPTION DE DONNEES, PROCEDE D'EMISSION DE
    CONTENU  AUDIOVISUEL,  PROCEDE  DE  RECEPTION  DE  CONTENU AUDIOVISUEL,
    EMETTEUR  DE  CONTENU AUDIOVISUEL, RECEPTEUR DE CONTENU AUDIOVISUEL, ET
    SUPPORT D'ENREGIS
PATENT ASSIGNEE:
  Matsushita Electric Industrial Co., Ltd., (1855508), 1006, Oaza-Kadoma,
    Kadoma-shi, Osaka 571-8501, (JP), (Applicant designated States: all)
INVENTOR:
  NISHIMURA, Takuya, 3-9-18-F, Matsuzaki-cho, Abeno-ku, Osaka-shi, Osaka
    545-0053, (JP)
  IITSUKA, Hiroyuki, 6-25-6, Kisaichi, Katano-shi, Osaka 576-0033, (JP)
  YAMADA, Masazumi, 6-24-10, Kinda-cho, Moriguchi-shi, Osaka 570-0011, (JP)
  GOTOH, Shoichi, 5-4-204, Myokenzaka, Katano-shi, Osaka 576-0021, (JP)
  TAKECHI, Hideaki, Lemonflats, R. 201, 11-10, Komatsu 4-chome,
    Higashiyodogawa-ku, Osaka-shi, Osaka 533-0004, (JP)
LEGAL REPRESENTATIVE:
  Grunecker, Kinkeldey,  Stockmair & Schwanhausser Anwaltssozietat (100721)
    , Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date):  EP 994599  A1  000419 (Basic)
                              WO 9950992  991007
APPLICATION (CC, No, Date):   EP 99910755 990330;  WO 99JP1606  990330
PRIORITY (CC, No, Date): JP 9889098 980401; JP 98161082 980609; JP 98162667
    980610
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS (V7):  H04L-009/08 ;  H04L-009/14 ;  H04L-009/32
  ; H04H-001/00
ABSTRACT WORD COUNT: 188
NOTE:
  Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:
Available Text  Language    Update    Word Count
      CLAIMS A  (English)  200016      3005
      SPEC A    (English)  200016     16016
Total word count - document A         19021
Total word count - document B             0
Total word count - documents A + B    19021

INTERNATIONAL PATENT CLASS (V7):  H04L-009/08 ...

... H04L-009/14 ...

... H04L-009/32
```

...SPECIFICATION receiving the AV contents.

A transmission device for transmitting such AV contents encrypts AV contents **before** transmission to protect the AV contents. A reception **device** receives and **decrypts** the encrypted AV contents, and displays the AV contents on the monitor.

As described above...key Kc to the VTR device 2 (steps S3 and S4). At this time, the **identifier** transmission means 16 **transmits** the **identifier** L corresponding to the **transmitted** control key Kc to the **identifier** recognition means 25. On the VTR device 2 side, the reception side **authentication** and **key** exchange means 23 transmits the **received** control key Kc to the key restoration means 22, and the **identifier** recognition means 25 **transmits** the received **identifier** L to the identifier storage means 26 and stores it therein (step S5). At this... reception process can be performed on the identifier L without the encryption process, etc., the **identifier** L is transmitted and **received** **before** performing the **authentication** and **key** exchange process which requires a heavy load on a system, and then it is determined...the processes in the procedure shown in FIG. 6 are performed.

That is, since an **identifier** L can be transmitted or received without an encryption process, etc., the **identifier** L is **transmitted** or **received** **before** performing the **authentication** and **key** exchange process which brings a heavy load onto the system, and it is then determined...

28/3,K/13 (Item 13 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00968334
Information recording apparatus, information reproducing apparatus, and information distribution system
Informationsaufzeichnungs- und -wiedergabegerat sowie Informationsverteilungssystem
Appareil d'enregistrement d'informations, appareil de reproduction d'informations, et systeme de distribution d'informations

PATENT ASSIGNEE:
KABUSHIKI KAISHA TOSHIBA, (213137), 72, Horikawa-cho, Saiwai-ku, Kawasaki-shi, Kanagawa 210-8520, (JP), (Applicant designated States: all)

INVENTOR:
Kambayashi, Toru, c/o Kabushiki Kaisha Toshiba, Intell. Prop. Div., 1-1 Shibaura 1-chome, Minato-ku, Tokyo 105-8001, (JP)
Akiyama, Koichiro, c/o Kabushiki Kaisha Toshiba, Intell. Prop. Div., 1-1 Shibaura 1-chome, Minato-ku, Tokyo 105-8001, (JP)
Tsujimoto, Shuichi, c/o Kabushiki Kaisha Toshiba, Intell. Prop. Div., 1-1 Shibaura 1-chome, Minato-ku, Tokyo 105-8001, (JP)
Sumita, Kazuo, c/o Kabushiki Kaisha Toshiba, Intell. Prop. Div., 1-1 Shibaura 1-chome, Minato-ku, Tokyo 105-8001, (JP)
Hirakawa, Hideki, c/o Kabushiki Kaisha Toshiba, Intell. Prop. Div., 1-1 Shibaura 1-chome, Minato-ku, Tokyo 105-8001, (JP)
Sugaya, Toshihiro, c/o Kabushiki Kaisha Toshiba, Intell. Prop. Div., 1-1 Shibaura 1-chome, Minato-ku, Tokyo 105-8001, (JP)

LEGAL REPRESENTATIVE:
Henkel, Feiler, Hanzel (100401), Mohlstrasse 37, 81675 Munchen, (DE)

PATENT (CC, No, Kind, Date): EP 878796 A2 981118 (Basic)
EP 878796 A3 000524
APPLICATION (CC, No, Date): EP 98108638 980512;
PRIORITY (CC, No, Date): JP 97122511 970513; JP 9816618 980129
DESIGNATED STATES: DE; NL
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): G11B-020/00; **G06F-001/00** ; **H04L-009/00**
ABSTRACT WORD COUNT: 143
NOTE:
Figure number on first page: 1+8

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9847	2220
SPEC A	(English)	9847	55951
Total word count - document A			58171
Total word count - document B			0
Total word count - documents A + B			58171

...INTERNATIONAL PATENT CLASS (V7): **G06F-001/00** ...

... **H04L-009/00**

...SPECIFICATION S43). The decoder unit 103 decodes the license information using the decoding key kd stored **in advance** to obtain the license condition (expiration date) and the **decoding key** kd(1). It is decided on the basis of the license condition (expiration date) whether... reproducing the contents information or the like.

In this case, the contents information is encrypted **in advance** . The

decoding key (to be referred to as a contents **decoding** **key** hereinafter) is added to the license information together with the contents license condition such as...banking system 2060 through a predetermined communication line to confirm fee payment, and the flow **advances** to processing in a contents **decoding** **key** acquisition section 2054 (step S1085).

The contents decoding key acquisition section 2054 searches a contents ...to prompt the user to select the identification number of period. The card IF 4001 **transfers** the request **key** **identification** information and **verification** **key** number to the **decoding** decision card. Upon **receiving** these pieces of information, the decoding decision card transfers one of the master keys KP...defined among a license generation device, a license update device, and a license decision unit **in** **advance** .

The entire license information is encrypted using a predetermined **decoding** **key** . The license information is decoded using a secret key held in a license decision unit...decoding the disk information by the card adapter 5004 which holds a decoding key kd **in** **advance** , the risk of disk **key** **decoding** midway along the distribution route by tapping or the like can be lowered.

The license...5003 stores the decoding key KpL corresponding to the encryption key KsL in the memory **in** **advance** . The encryption parameter update information UL is **decoded** using the decoding **key** KpL to update the encryption parameters X(l), Pl, Prl, X(k), Pk, and Prk...

...P stores the decoding key KpC corresponding to the encryption key KsC in the memory **in** **advance** . The encryption parameter update information UC is **decoded** using the decoding **key** KpC to update the encryption parameters X(k), Pk, and Prk stored in the common...5004 stores the decoding key KpA corresponding to the encryption key KsA in the memory **in** **advance** . The encryption parameter update information UA is **decoded** using the decoding **key** KpA to update the encryption parameters X(l), Pl, Prl, X(k), Pk, Prk, X...

...5005 stores the decoding key KpD corresponding to the encryption key KsD in the memory **in** **advance** . The encryption parameter update information UD is **decoded** using the decoding **key** KpD to update the encryption parameters X(D), PD, and PrD stored in the base...

28/3,K/16   (Item 16 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00683558
Software pay per use system
Softwaresystem mit Bezahlung zu Benutzung
Systeme de logiciel payant par utilisation
PATENT ASSIGNEE:
  AT&T Corp., (589370), 32 Avenue of the Americas, New York, NY 10013-2412, (US), (Applicant designated States: all)
INVENTOR:
  Michel, Alan D., 522 Concord Ct., Fishers, Indiana 46038, (US)
  Reinke, Robert E., 12340 Buck Court, Indianapolis, Indiana 46236, (US)
LEGAL REPRESENTATIVE:
  Buckley, Christopher Simon Thirsk et al (28912), Lucent Technologies (UK) Ltd, 5 Mornington Road, Woodford Green, Essex IG8 0TU, (GB)
PATENT (CC, No, Kind, Date): EP 653695 A2 950517 (Basic)
                              EP 653695 A3 000322
APPLICATION (CC, No, Date):   EP 94308083 941102;
PRIORITY (CC, No, Date): US 152769 931115
DESIGNATED STATES: DE; ES; FR; GB
INTERNATIONAL PATENT CLASS (V7): **G06F-001/00**
ABSTRACT WORD COUNT: 112
NOTE:
  Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPAB95	2457
SPEC A	(English)	EPAB95	4793
Total word count - document A			7250
Total word count - document B			0
Total word count - documents A + B			7250

INTERNATIONAL PATENT CLASS (V7): **G06F-001/00**

...CLAIMS capable of decrypting said identified secured software;
said software user system further comprising:
means for **transmitting** said secured software **identification** to the software validation system over said communications network,
means for **receiving** said chosen **decryption** **key** capable of **decrypting** said identified secured software from said software validation system over said communications network, and
means...
...chosen decryption key.
2. A software validation system comprising:
means for storing at least one **decryption** **key** ;
means for **receiving** from a communications network an identification of encrypted software;
means for recording the receipt of said **identification** ; and
means for **transmitting** to the communications network a decryption key chosen from said at least one stored decryption...

...for the execution of secured software, the system comprising:
encrypted computer program code;
means for **transmitting** an **identification** of the encrypted computer program code to a communications network;
means for **receiving** a **decryption** **key** from the

communications network, said decryption key capable of decrypting said encrypted computer program code...The software user computer system of claim 14 wherein said masked decryption key is encrypted **prior** to receipt, said system further comprising means for **decrypting** said encrypted masked **key** prior to unmasking said key.

17. The software user computer system of claim 14 wherein said second random number is encrypted **prior** to receipt and said masked **decryption key** is encrypted **prior** to receipt, said system further comprising:
   means for **decrypting** said encrypted masked **key prior** to unmasking said **key** ; and
   means for **decrypting** said encrypted second random number prior to combining said first random number and second random...

...validation system;
   masking said decryption key with a random number in said software validation system **prior** to transmitting the **decryption key** to the user; and
   unmasking said decryption key with said random number in the user...

...A method for validating secured computer software comprising the steps of:
   storing at least one **decryption key** ;
   receiving from a communications network an identification of encrypted software;
   recording the receipt of said **identification** ; and
   transmitting to the communications network a decryption key chosen from said at least one stored decryption a communications network which results in a service fee;
   transmitting an **identification** of the secured software to the communications network;
   receiving a **decryption key** from the communications network, said decryption key capable of decrypting said secured software; and
   decrypting...

...service fee.

38. The method of claim 36 wherein said masked decryption key is encrypted **prior** to receipt, said method further comprising the step of **decrypting** said encrypted masked **key** prior to unmasking said key.

39. The method of clairn 36 wherein said second random number is encrypted **prior** to receipt and said masked **decryption key** is encrypted **prior** to receipt, said method further comprising the steps of:
   decrypting said encrypted masked **key prior** to unmasking said **key** ; and
   decrypting said encrypted second random number prior to combining said first random number and second random...

28/3,K/22 (Item 22 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00268335 **Image available**
SOFTWARE EVAULATION AND DISTRIBUTION APPARATUS, SYSTEM, AND METHOD
PROCEDE, SYSTEME ET APPAREIL D'EVALUATION ET DE DISTRIBUTION DE LOGICIELS
Patent Applicant/Assignee:
INFONOW CORPORATION,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9416508 A1 19940721
Application: WO 94US97 19940106 (PCT/WO US9400097)
Priority Application: US 931262 19930107
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AU CA JP NZ AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE
Publication Language: English
Fulltext Word Count: 24805

Main International Patent Class (v7): **H04L-009/00**
Fulltext Availability:
Detailed Description

Detailed Description
... apparatus also includes a key decoding device that decodes the coded key, using the user **identification** , to **provide** the key,
a reading device that reads the encrypted copy **received** from the central
office, a **decrypting** device that **receives** a read out of the encrypted copy
from the reading device, and uses the key...the return message transmitted by the central office in response to the incoming message is **received** . The **coded** **key** is **decoded** , using the user **identification** , to **provide** the key. The encrypted copy received from the central office is read, and
the encrypted...of the test is FALSE,
the desktop vending module returns to step 155. Otherwise it **advances** to
step 157, where it **decodes** the **coded** **key** for the product selected, The
desktop vending module retrieves the coded key and the user...

```
33/3,K/2     (Item 2 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2006 European Patent Office. All rts. reserv.

01130512
METHOD  AND  APPARATUS  FOR  SECURE  COMMUNICATION OF INFORMATION BETWEEN A
    PLURALITY OF DIGITAL AUDIOVISUAL DEVICES
VERFAHREN  UND VORRICHTUNG ZUR GESCHUTZTEN INFORMATIONSUBERTRAGUNG ZWISCHEN
    EINER VIELZAHL DIGITALER AUDIOVISUELLER GERATE
PROCEDE ET DISPOSITIF D'ECHANGE SECURISE D'INFORMATIONS ENTRE UNE PLURALITE
    D'APPAREILS AUDIOVISUELS NUMERIQUES
PATENT ASSIGNEE:
  Canal+ Technologies, (3376171), 34, Place Raoul Dautry, 75015 Paris, (FR)
    , (Proprietor designated states: all)
INVENTOR:
  DAUVOIS, Jean-Luc, 19, rue Eugene Manuel, F-75116 Paris, (FR)
  BENARDEAU, Christian, 13, allee des Puisatiers, F-77600 Bussy Saint
    Georges, (FR)
LEGAL REPRESENTATIVE:
  Santarelli (100891), 14, avenue de la Grande Armee, 75017 Paris, (FR)
PATENT (CC, No, Kind, Date):  EP 1099348  A1  010516 (Basic)
                              EP 1099348  B1  021016
                              WO 2000004718  000127
APPLICATION (CC, No, Date):   EP 99929648 990714;  WO 99IB1323  990714
PRIORITY (CC, No, Date): EP 98401778 980715; EP 98401870 980722
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI;
  LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): H04N-007/167;  H04L-029/06
NOTE:
  No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text  Language   Update    Word Count
      CLAIMS B  (English)  200242     1430
      CLAIMS B   (German)  200242     1501
      CLAIMS B   (French)  200242     1574
      SPEC B    (English)  200242    10449
Total word count - document A           0
Total word count - document B        14954
Total word count - documents A + B   14954

...INTERNATIONAL PATENT CLASS (V7):  H04L-029/06

...SPECIFICATION B1
    The present invention relates to a method and apparatus for  secure
  communication of  information  between a plurality of digital audiovisual
  devices connected in a  network .
    The present invention is particularly applicable to the field of
  digital television, where scrambled audiovisual...session key and
  thereafter descrambles an associated transmission or programme for
  display.
    In one embodiment,  prior  to the communication of the first
  certificate , the second  device   receives  a secondary system
  certificate comprising the management public key encrypted by a system
  private key, the second device decrypting the system certificate using a
  system public key so as to  obtain  the management public  key  used
  thereafter to  decrypt  the  encrypted  transport public  key .
    This embodiment may be implemented, for example, where a different
  source for the first and...
```

33/3,K/7 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00545536 **Image available**
SYSTEM FOR TRACKING END-USER ELECTRONIC CONTENT USAGE
SYSTEME POUR SUIVRE L'UTILISATION DE CONTENUS ELECTRONIQUES PAR UN UTILISATEUR FINAL

Patent Applicant/Assignee:
INTERNATIONAL BUSINESS MACHINES CORPORATION,
DORAK John Jr,
DOWNS Edgar,
GRUSE George Gregory,
HURTADO Marco,
LEHMAN Christopher,
LOTSPIECH Jeffrey,
MEDINA Cesar,
MILSTED Kenneth,

Inventor(s):
DORAK John Jr,
DOWNS Edgar,
GRUSE George Gregory,
HURTADO Marco,
LEHMAN Christopher,
LOTSPIECH Jeffrey,
MEDINA Cesar,
MILSTED Kenneth,

Patent and Priority Information (Country, Number, Date):

Patent:	WO 200008909 A2 20000224 (WO 0008909)
Application:	WO 99US18383 19990812 (PCT/WO US9918383)
Priority Application:	US 98133519 19980813; US 98177096 19981022

Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE
GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK
MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN
YU ZA ZW AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE

Publication Language: English
Fulltext Word Count: 51208

Main International Patent Class (v7): **G06F-001/00**
International Patent Class (v7): **H04L-029/06** ...

... **G06F-017/60**

Fulltext Availability:
Detailed Description
Claims

English Abstract
...system for tracking usage of digital content on user devices. Electronic stores coupled to a **network** sell licenses to play digital content **data** to users. A system for **securely** providing **data** , the system being capable of receiving both data encrypted with a first encryption key and...

Detailed Description
... I 0 from AT&T, Liquid Audio Pro from Liquid Audio Pro Corp., City Music **Network** from Audio Soft and others offer transmission of digital **data** over **secured** and unsecured electronic **networks** . The use of

secured electronic **networks** greatly reduces the requirement of digital content providers of distributing digital to a wide audience...Snyder, David Maher, of AT&T Labs, Florham Park, N.J. available online URL http:// **www** .a2bmusic.com/about/papers/musicipp.htm. Cryptographically protected **container** , called DigiBox, in the article " **Securing** the Content, Not the Wire for Information Commerce" by Olin Sibert, David Bernstein and David...be secure or trusted. Therefore allowing transmission over network infrastructures such as the Web and **Internet** . This is due to the fact that the Content is **encrypted** within **Secure Containers** and its storage and distribution are separate from the control of its unlocking and use...

Claim
... data decrypting key to a second system.

8 The system of claim 7, wherein the **encrypted data decrypting key** is **received** from another system.

9 The system of claim 8, further comprising authorization for the data **prior** to transferring the encrypted data **decrypting key** to a second system.

10 A system for managing content data, associated metadata, and associated...

51/3,K/2 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00419920 **Image available**
TRUSTED INFRASTRUCTURE SUPPORT SYSTEMS, METHODS AND TECHNIQUES FOR SECURE ELECTRONIC COMMERCE, ELECTRONIC TRANSACTIONS, COMMERCE PROCESS CONTROL AND AUTOMATION, DISTRIBUTED COMPUTING, AND RIGHTS MANAGEMENT
SYSTEME D'ASSISTANCE INFRASTRUCTURELLE ADMINISTRATIVE, PROCEDES ET TECHNIQUES SURES CONCERNANT LE COMMERCE ET LES TRANSACTIONS ELECTRONIQUES, COMMANDE ET AUTOMATISATION DES PROCESSUS COMMERCIAUX, CALCUL REPARTI ET GESTION DES REDEVANCES

Patent Applicant/Assignee:
INTERTRUST TECHNOLOGIES CORP,
SHEAR Victor H,
VAN WIE David M,
WEBER Robert,

Inventor(s):
SHEAR Victor H,
VAN WIE David M,
WEBER Robert,

Patent and Priority Information (Country, Number, Date):

Patent:	WO 9810381 A1 19980312
Application:	WO 96US14262 19960904 (PCT/WO US9614262)
Priority Application:	WO 96US14262 19960904

Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IL IS JP
KE KG KP KR KZ LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD
SE SG SI SK TJ TM TR TT UA UG US UZ VN KE LS MW SD SZ UG AM AZ BY KG KZ
MD RU TJ TM AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF
CG CI CM GA GN ML MR NE SN TD TG

Publication Language: English
Fulltext Word Count: 85684

...International Patent Class (v7): **G06F-17:60**
Fulltext Availability:
Detailed Description
Claims

English Abstract

...usage clearing, secure directory services, and other transaction related capabilities functioning over a vast electronic **network** such as the **Internet** and/or over organization internal Intranets. These administrative and support services can be adapted to...

...reuse these services in response to competitive business realities. A Distributed Commerce Utility having a **secure** , **programmable** , distributed architecture provides administrative and support services. The Distributed Commerce Utility makes optimally efficient use...

...of its participants. Different support functions can be collected together in hierarchical and/or in **networked** relationships to suit various business models and/or other objectives. Modular support functions can be...

French Abstract

...repertoires, et autres prestations liees aux transactions traitees par un vaste reseau electronique tel qu' **Internet** et/ou par des Intranets internes a des organisations. Ces services peuvent etre adaptes aux...

Detailed Description

TRUSTED INFRASTRUCTURE SUPPORT SYSTEMS,
METHODS AND TECHNIQUES FOR
SECURE ELECTRONIC COMMERCE, ELECTRONIC
TRANSACTIONS, COMMERCE PROCESS CONTROL
AND AUTOMATION, DISTRIBUTED COMPUTING, AND
RIGHTS MANAGEMENT
Field...

...the Inventions

These inventions generally relate to optimally bringing the efficiencies of modem computing and **networking** to the I 0 administration and support of electronic interactions and consequences and ftirther relate to a **secure** architecture enabling distributed, trusted administration for electronic commerce.

These inventions relate, in more detail, to...

...administration,

electronic process control and automation, and clearing functions across and/or within an electronic **network** and/or virtual distribution environment; and/or clearing, control, automation, and other administrative, infrastructure and support capabilities that collectively enable and support the operation of an efficient, **secure** , peer-to-peer collection of commerce participants within the human digital community.

The Distributed Commerce Utility technologies provided by the present inventions provide a set of **secure** , distributed support and administrative services for electronic commerce, rights management, and distributed computing and process...
...of their operation.

The Distributed Commerce Utility can ensure appropriately high levels of physical, computer, **network** , process and policy-based security and automation while providing enhanced, efficient, reliable, easy to use...chain of handling and control,
B. secure, trusted intemodal communication and interoperability,
1 5 C. **secure** database,
D. authentication,
E. cryptographic,
F. fingerprinting,
G. other VDE security techniques,
H. rights operating system,
1. object design and **secure** **container** techniques,
J. **container** control structures,
K. rights and process control language,
L. electronic negotiation,
M. secure hardware, and...might be distributed in and/or throughout existing or new communications infrastructure or other electronic **network** support components.

Other support services might operate within secure execution spaces (e.g., protected processing...

...secure web of support service fabric.

24
Other support services might operate both in the **network** support infrastructure and at user electronic appliances.

Such distributed support services may complement (and/or...subsequently adapt (modify), any support service functions to any desired degree across a system or **network** provides great power, flexibility and increases in efficiency. For example, distributing
27
aspects of support...administrative support for any or all of the following.

e trusted electronic event management,
o **networked** , automated, distributed, **secure** process administration and control,
o Virtual Distribution Environment chain-of-handling and control, and
o...

...event) management
29

(e.g., auditing, control, rights fulfillment, etc.), across and/or within electronic **networks** , including 4 Cunconnected," virtually connected, or periodically connected **networks** .

The Commerce Utility Systems may govern electronic process chains and electronic event consequences related to...

...activities,
compiling, aggregating, using and/or providing information relating to use of one or more **secure containers** and/or content and/or processes (events), including contents of **secure containers** and/or any other content,
providing information based upon usage auditing, user
30
I E...io/pule '2uilgoid
Z9Ztll/96Sfl/1Jd ISCOT/96 OM
Systems further support distributed, scaleable, efficient **networked** and/or hierarchical fixed and/or virtual clearinghouse models which employ secure communication among a...appliance I 00 electronically connected to Distributed Commerce Utility 75. In this example, an electronic **network** 150 connects appliancc I 00 to Distributed Commerce Utility 75. Distributed Commerce Utility 75 supports...

...from television
39
broadcasters I IO and/or satellites 1 12 via a cable television **network** II 4, for example. Player/recorder 104 could play various types of program material from...

...may be based on
one or more computer chips, such as a hardware and/or **software** based " **secure** processing unit" as shown in Figure 9 of the Ginter et al. Patent specification. The...may insist upon the protected processing environment 154 providing a copy protection mechanism 120 that **securely** protects against copying video **program** 102a. Distributed Commerce Utility 75 may include a special purpose Commerce Utility System 90c called...addition, some of the functions of the Commerce Utility System 90 may be distributed within **network** 150 - for example, in the equipment used to communicate data between appliances 100.

Distributing Multiple...other administrative and support service functions (for example, issuance of important digital certificates, maintaining massive **data** bases supporting **secure** directory services, etc.) are much more centralized. The degree of distributedness of any particular administrative...comprise a vast "web" of distributed, partly distributed and/or centralized Commerce Utility Systems 90. **Network** 150 can be used to connect this web of Commerce Utility Systems 90 to a...

...appliances I 00 that can all share the

Distributed Commerce Utility 75. For example, electronic **network** 150 can connect to.

set top boxes 106 and/or media players 104,
personal computers...

...appliances I 00
including for example, manufacturing control device, household appliances, process control equipment, electronic **networking** and/or other communication infrastructure devices, mainframe and/or mini computers, etc.

In this example...

...4A shows that the web of Commerce Utility Systems may be vast or limitless. Indeed, **network** 150 may be a seamless web stretching around the world and connecting millions upon I...user appliances I 00 are shown as standing up rectangular columns in the diagram. Electronic **network** 150 is shown as a road which connects the various Commerce Utility Systems to one...
...consumer electronic appliances
I 00. Electronic digital containers 152 may be carried along this electronic **network** or "information highway" 150 between different electronic installations.

I 0 Figure 7A illustrates just some...this example, financial clearinghouse 200 may
communicate with appliance protected processing environment 154 over electronic **network** 150 in a **secure** manner using electronic **containers** 152 of the type described, for example, in the Ginter et al. patent specification in...

...clearinghouse 200 may receive payment
65
information 202 from protected processing environment 154 in these **secure** **containers** 152, and interact electronically or otherwise with various banking, credit card or other financial institutions...to consumers 95 -- for example, by transmitting the statements to appliance I 00 in a **secure** electronic **container** 152b to preserve the confidentiality of the statement information. In this example, consumers 95 can...
...example, the payment mechanism II 8 provided by protected processing environment 154 might be an **electronic** **wallet** supplying **electronic** money for use in paying for electronic services or content. This **electronic** **wallet** may hold money in digital form. Consumers 95 can spend the digital money on whatever they wish. When the **electronic** **wallet** is empty,
66
L9
Xaql j! 'snuinsuoo oqjL -iaqjaBojjp jjo pouinj 2uioq oi papplop @Z...
viewing habits consistent with protecting the
consumers' privacy. These reports can also be sent within **secure** **containers** 152. For example, usage clearinghouse 300 might provide a summary report 304b to advertisers 306...

...154 by
delivering permissions (control sets) 188 in response.

For example, suppose that consumers 95 **want** to watch a concert or a fight on television set 102. They can operate their...

...program. Protected processing environment 154 may automatically contact rights and permissions clearinghouse 400 over electronic **network** 150 and send an electronic request 402.

The rights and permissions clearinghouse 400 can "look...price for watching the program (for example,
$5.95 to be deducted from the consumers' **electronic** **wallet**).

I 0 Appliance I 00 can ask the consumers 95 if they **want** to pay $5.95 to watch the program. If they answer "yes" (indicated, for example, by operating remote control 108), the appliance I 00 can automatically debit the consumers' **electronic** **wallet** and "release" the program so the consumers can watch it.

1 5 Rights and permissions clearinghouse 400 can deliver permissions 188 within a **secure** **container** 152b that may optionally also contain the information controlled by the permissions -- or permission 188...

...content travels to
the appliance I 00. For example, the permissions could be sent over **network** 150, whereas the program it is associated with may arrive directly from satellite 1 12 or over some other path such as cable television **network** II 4 (see Figure 1).
Rights and permissions clearinghouse 400 may also issue reports 406...computerized telephone or name services directory. Consumers
95 can send a request 602 specifying the **information** they need.

Secure directory services 600 can "look up" the information and provide the answer 604 to consumers...

...Commerce Utility Systems 90 to
1 5 perform its tasks.

For example, suppose consumers 95 **want** to electronically order a pizza from Joe's Pizza. They decide what kind of pizza they **want** (large cheese pizza with sausage and onions for example). However, they don't know Joe...

...phone number).

Consumers 95 can use remote control 108 to input information about what they **want** to have looked up ("Joe's Pizza, Lakeville, Connecticut"). Protected processing environment 154 may generate a request 602 containing the identification **information** and send this request to **secure** directory services 600. It can send the request in a **secure** **container** 152a.

7.3
ft

OuOOwOs j! OIBO lOu @uw @6 sioLunsuoo aql 'XOUAiid siatunswo z)qi...control 1 08 to select the particular seller, style and color of a sweater they **want** to order at a particular price. In this home shopping example, appliance I 00's...preferred embodiment, provide a variety I 0 of electronic maintenance and other functions to keep **network** 150, appliance I 00 protected processing environments 154 and Distributed Commerce Utility 75 operating securely, smoothly and efficiently. For example, VDE administrator 800 may manage cryptographic **keys** used for electronic **security** throughout 1 5 **network** 150, and may also provide services relating to the maintenance of **secure** **data** by appliances I 00, the various Commerce Utility Systems 90, and other electronic appliances.

As...OAA, compartmentalized, services-based, "component" oriented, distributed multi-processing operating system environment that integrates VDE **security** control **information** , components, and protocols with traditional operating system concepts. The preferred example Commerce Utility System 90...service function 90-2 or service application component 90-3 throughout a system 50 or **network** - including for example to electronic appliances of individual consumers 95. Figure 17F shows an example...but the processing can instead be done on the local consumer electronic appliance, on a **networked** appliance.

Distributing support services in this manner provides additional capabilities that may not be present...

...permissions previously requested by the organization. Such a local rights and permissions clearinghouse could reduce **network** traffic and provide a convenient local repository for organization-specific permissions (e.g., site licenses...and/or customer and/or other user accounts for funds, credits and debits.

9 Using **secure** **containers** in any step, part, or process of providing secure financial clearing services.

* Controlling secure financial...107 activity and the periodic passing of information related to such activity through a clearinghouse **network** for further processing and/or accumulation.

Efficiently measuring and managing micro-payment activity while minimizing...peer relationships with, one or more of said clearinghouses.

Distributing financial clearing functions across a **network** or other system (for example, every consumer or other value chain participant node can perform...200 and/or other secure or insecure protected processing environments., permitting the financial clearinghouse to **securely** share state and update **information** with other Commerce Utility Systems or other participants.

In the example shown, the payment information 202 (which may arrive in one or more **secure containers** 152) is the primary input to payment processing block 208. If desired, payment
116
L...electronic appliances I 00(l) ... 1 OO(N). Such communications may be by way of **secure** digital **containers** 152.

It is desirable for most Commerce Utility Systems 90 (including financial clearinghouse 200) to...to store information used to track encumbrances as well.

There may also be sets of **security information** used to communicate with protected processing environments and/or users employing the protected...may provide the summary report 240 to provider 164 by transmitting it electronically within a **secure container** 152c. Financial clearinghouse 200 may also coordinate with a financial intermediary 258 and one or...or the like, to the consurnerls electronic appliance by transmitting it within one or more **secure containers** 152b. The consumer may operate his or her electronic appliance I 00 to open the...clearinghouse 200. This payment may be in the form of electronic currency packaged within a **secure** electronic **container** 152a, or it might be in some other form (e.g., reported usage information coupled...authorization 152a and these payment
controls 188a to financial clearinghouse 200 within one or more **secure** electronic **containers** 152a.

Financial clearinghouse 200 processes the payment or
1. ...repackager 174 may create the latest issue of the newsletter and distribute it in a **secure** electronic **container** for reading by customer 95. In this example, the **secure** electronic **container** 152a may **contain** at least four separately "delivered" sets of business requirements -- one for each of the three...

...works and/or the controls applying to them can be sent and delivered in independent **secure containers** 152, and/or some or all of the works and/or controls may be located...

...duplication and redistribution. This pass-along problem is serious in digital environments such as the **Internet** .

The virtual distribution environment disclosed in the Ginter et al.

patent specification and the administrative...individual transactions that need to be cleared, and decreasing messaging traffic over electronic **network** 150. Of course, payment aggregation is not necessarily suitable for every transaction (some large, critical...at lest one further clearinghouse and/or value chain rightsholder; and wherein said clearinghouse may **securely** provide differing derived usage **information** to different other parties who have a clearinghouse role or other rightsholder role...interested parties and/or to the public, thereby laying the foundation for truly trusted, commercial **networks** .

Allowing value chain participants, including, for example, commercial publishers and distributors, and/or consumers and...more classes derived from usage data created, collected, transmitted, in conjunction with at least one **secure** **container** and/or VDE in the preferred embodiment.

Supporting advertising and marketing, including supporting...clearing (e.g., for efficiency and/or other reasons).

Distributing usage clearing functions across a **network** or other system (for example, every consumer and/or other value chain participant...

...senior usage clearinghouse.

Distributing and/or otherwise authorizing usage clearing functions across a system or **network** , for example, where every consumer and/or certain or al I other value chain participant...Communication between usage clearinghouse 300 and other electronic appliances 100 may be by way of **secure** electronic **containers** 152, if desired. As explained in more detail in connection with financial clearinghouse 200, usage...

...usage clearinghouses 300) and/or to provide a distributed database across a number of secure **network** protected processing environments or electronic appliances.

Data aggregation 324 and analysis 328 may be used...to the ones they themselves are distributing. Consumer 95, on the other hand, may not **want** to reveal this detailed information about all of the software programs that are ...on his or her personal computer.

As another example, digital broadcast rights holders 164 may **want** to know about every broadcasted program that 166 consumer 95 watches, whereas the consumer may not **want** anyone else to know the kinds of programs he or she is interested in.

Usage...

...big discount in return for allowing full disclosure of usage information.

Some secretive consumers may **want** the outside world to know as little as possible about their usage habits and will...

...consumers may not care what the outside world knows about their usage habits, and will **want** to take advantage of large discounts based upon more full disclosure. Any number of such...

...precisely what kinds of information are revealed and which ones
are kept secret. Because usage **data** is being collected within a
secure protected processing environment 154 that is part of the
consurnerts electronic appliance I 00, the consumer can be
167
confident that the usage **data** will be **securely** handled and that
unauthorized disclosure will not occur without his or her consent.

Based, for...and securely provide to
one or more rights and permissions clearinghouse
ways in which they **want** their intellectual property
products (for example, VDE protected digital
properties) to be used and not...associated information
and/or electronic control processes and thereby
avoiding user frustration and inefficiency).

Using **secure** **containers** such as those described in
I 0 Ginter, et al., in any step, part, or...

...including, for example,
digital information describing and/or governing control
processes (e.g., event management **information**)
managed through, for example, **secure** VDE chain of
handling and control.

Distributing rights clearing functions across a **network** or
other system (for example, every consumer and/or other
174
value chain participant node...senior rights clearinghouse
distributing and/or otherwise authorizing rights clearing
functions across a system or **network** , for example,
where every consumer and/or certain or all other value
chain participant nodes...

...its own,
secure rights clearing transactions and function in the
context of the overall clearinghouse **network** , including,
clearinghouse interoperation with one or more other
participants interoperable nodes, and as elsewhere in...

...to queries, rights
and permissions clearinghouse 400 provides
permissions 188 together with associated prices in
secure electronic **containers** 152. The permissions
controls 188 may be provided independently of the
content.

I 0 Negotiatedpermissions...438 may
perform the registration function 419. Secure communications
facility 430 communicates securely over electronic **network** 150
with consumers 95, authors 164, publishers 168, aggregators 170,
181
repackagers 174, and other value chain participants via **secure**
containers 152. Authenticator 434 and authorization checker 436
perform authentication functions as the Ginter et al...clearinghouse 400
and the government
agency 440 may, for example, make use of VDE and **secure**

containers 152.

Figures 44A-44E show an additional rights and permissions clearing process that may be...on physical evidence in addition to automatic
services for issuing dependent certificates.

May use public **key** cryptography, private **key** , and/or **secure** VDE virtual **networks** to support, e.g. create, digital certificates.

Can issue certificates that support the context for...

...profiles and/or rules and controls.

Distributing revocation list information among interoperable, peer-to-peer **networked** , Distributed Commerce Utility nodes on a time based, other event based manner, wherein information is...

...of handling
and control embodied in electronic control sets.

Distributing certificate authority functions across a **network** or other system (for example, every
...certificate authority clearinghouse distributing and/or otherwise authorizing rights clearing functions across a system or **network**
196
Every consumer and/or certain or all other value chain participant nodes can potentially...
...service
initiating its own, secure certificates and function in the context of the overall clearinghouse **network** , including, clearinghouse interoperation with one or more other participants interoperable nodes, and as elsewhere in...

Claim

... electronic appliance (I 00),
5, a second electronic appliance (I 00'), and
an electronic communications **network** (I 50) that allows the
first and second electronic appliances (I 00, I 00') to...

...least one of the first and second electronic appliances (I 00, I 00')
through the **network** (I 50), the third
electronic appliance performing a third part of the clearing operation.

12...and/or rights management system as in
claim I further characterized in that the electronic **network** (I 50)
couples the first and second electronic appliances (I 00, I 00') to a I
further characterized in that that clearing operation includes **securely**
I 0 providing directory **information** .

27 An electronic commerce and/or rights management system as in
claim I further characterized...

...remote clearinghouse nodes in
response to at least a portion of said local store of **information** and
rules and controls **securely** and separately supplied by said
clearinghouse arrangement and at least one third party digital
information...

...an end-user
participant commerce node; and
d. Enabling said end-user participant node to **securely** , separately
receive
rights permission **information** from said remote rights repository to, at
least in part, enable a desired usage of to
support end-user electronic commerce activity;
C. **Securely** conveying digital **information** between end-user
commerce appliances and at least one commerce utility system;
d. **Securely** conveying digital **information** between two or more of
said commerce utility systems; and
e. **Securely** conveying digital **information** between two or more of
said end-user commerce appliances.

19 A method for supporting...

...Providing plural system services through use of said plural service
arrangements for use by digital **information** rightsholders; and
d. **Securely** supporting electronic commerce at a value chain participant
node at least in part through the...

...plural.
separate authorized commerce service providers and plural authorized
end-users; and
d. Transferring digital **information** **securely** between one or more end
user sites and plural, separate commerce service providers in response...

...said
value chain participants.

AMENDED SHEET (ARITICLE 1 9)
. A method for exchanging digital **information** within a distributed, **secure** , electronic commerce arrangement, comprising the steps of
a. Establishing unique identities for participants within an...

...comprise commerce
utility service providers, product and/or information service providers, and product and/or **information** service users;
b, **Securely** delivering a first type of digital information between an arrangement participant A and an arrangement...
...C and arrangement participant D; and
e. Protecting participant rights at least in part through **programmable** , **secure** , rules and controls based governance of use of said types of digital information delivered to...at least in part through use of said unique site
identifier, software installation and/or **software** updating;
d. **Securely** associating rules and controls with certain digital **information** : e. **Securely** distributing said digital **information** for use at said end-user
electronic commerce installations; and
f. Controlling use of at...

...the steps of.
a. Monitoring usage of digital information at distributed electronic commerce nodes;
b. **Securely** communicating **information** related to said monitored usage from at least one of said commerce nodes to at...

...based, at least in part, on
control information provided by a first party; and
c. **Securely** reporting **information** reflecting said commerce node auditing
of usage information from said commerce node to a commerce...and
c. Governing, at least in part, said distributed commercial process through the use of **secure** control **information** contributed by said transaction authority and, at least in part, through the use of peer...

...said method comprising the steps of.
a. Employing distributed checkpoint electronic switches in a communications **network** ;
b. Communicating through said **network** , at least in part **secured** digital
information provided by a first commercial party, said **secured** digital
information to be at least in part received by at least one of said checkpoint electronic switches;
c. Interacting with at least a portion of said received **secured** **information**
through operation of at least one of said checkpoint electronic switches to: (1) acquire **information** related to said **secured** **information** . and/or
(2) certify, authenticate, validate, and/or otherwise assert and/or test said information...
...provide a trusted commerce service; and
d. Further communicating at least a portion of said **secured** digital **information** from said distributed checkpoint electronic switch to a second, remotely located commercial party different from said first

commercial party.
AMENDED SNET (ARTICLE 19)
. A method for operating a digital broadcasting **network** . said method comprising the steps of
a) **Securely** providing digital **information** to plural participants in a cooperative arrangement of **network** information hosting and/or other service parties;
b) Basing variables related to said digital information...

...for supporting a secure messaging system, said method comprising the steps of. a. Packaging digital **information** at least in part **securely** in an electronic **container** for transmission by a first party to at least one additional party;
b. Employing a...

...least one additional party;
d. Providing authentication for at least a part of said digital **information**
and/or for said **secure** **container** ; and
e. Preventing said first party from effectively denying that said first party sent at...trusted commerce utility system
hierarchically less senior than said first trusted commerce utility system;
c. **Securely** communicating control **information** between said first and second commerce utility systems;
d. Establishing trusted end-user commerce nodes...

...user commerce nodes, wherein said service operates at least in part in accordance with said **securely** communicated control **information** .

21 A method for supporting a virtual computer, said method compnsing the steps of.
a...

...at least in part. on said use rights information.

22 A method for supporting virtual, **networked** banking activities, said method comprising the steps of
a. Enabling plural banking arrangements that comprise a web of separately managed protected processing environments;
b. Communicating control **information** **securely** between plural of said separately managed protected processing environments;
c. Governing one or more banking...

...steps of
a. Enabling a financial clearinghouse employing at least one protected processing environment to **securely** receive payment related **information** from
...information including governing payment fulfillment at least in part based upon electronic rights
management control **information** processed ; and
d. **Securely** communicating payment fulfillment **information** to at least one of (1) a payment fulfillment organization, and (2) an intended recipient...

...a

```
 51/3,K/11     (Item 11 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2006 European Patent Office. All rts. reserv.

01674589
Financial process device
Vorrichtung fur finanzielle Verfahren
Dispositif de procedes financieres
PATENT ASSIGNEE:
  FUJITSU LIMITED, (211463), 1-1, Kamikodanaka 4-chome, Nakahara-ku,
    Kawasaki-shi, Kanagawa 211-8588, (JP), (Applicant designated States:
    all)
  Sumitomo Mitsui Banking Corporation, (4478420), 1-2, 1-Chome Yurakucho
    Chiyoda-ku,, Tokyo, (JP), (Applicant designated States: all)
INVENTOR:
  Mori, Nobuyuki, Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku,
    Kawasaki-shi, Kanagawa 211-8588, (JP)
  Morita, Michihiro, The Sakura Bank Limited, 3-1, Kudan Minami 1-chome,
    Chiyoda-ku, Tokyo 102-0074, (JP)
  Oki, Masanao, The Sakura Bank Limited, 3-1, Kudan Minami 1-chome,
    Chiyoda-ku, Tokyo 102-0074, (JP)
  Hirota, Takaaki, The Sakura Bank Limited, 3-1, Kudan Minami 1-chome,
    Chiyoda-ku, Tokyo 102-0074, (JP)
LEGAL REPRESENTATIVE:
  Stebbing, Timothy Charles et al (59643), Haseltine Lake, Imperial House,
    15-19 Kingsway, London WC2B 6UD, (GB)
PATENT (CC, No, Kind, Date):  EP 1376500  A2  040102 (Basic)
                              EP 1376500  A3  040107
APPLICATION (CC, No, Date):   EP 2003015540 980204;
PRIORITY (CC, No, Date): JP 9723776 970206
DESIGNATED STATES: CH; DE; GB; LI; NL
RELATED PARENT NUMBER(S) - PN (AN):
  EP 858057  (EP 98300799)
INTERNATIONAL PATENT CLASS (V7): G07F-019/00;  G06F-017/60 ; G07F-007/08
ABSTRACT WORD COUNT: 82
NOTE:
  Figure number on first page: 59

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text  Language    Update    Word Count
      CLAIMS A  (English)   200401      759
      SPEC A    (English)   200401    45715
Total word count - document A         46474
Total word count - document B             0
Total word count - documents A + B    46474
...INTERNATIONAL PATENT CLASS (V7):  G06F-017/60

...SPECIFICATION may arise with digital contents such as software, image
  data, etc. transmitted through a communications  network . That is, such
  intangible goods are subject to the risk that a purchaser may refuse...

...successfully delivered to the purchaser.
    When the above described digital contents are marketed through a
  network , there can be various risks such as an illegal use risk by the
  third party...
```

...is the most effective method for reducing the above described risks. However, since the present **encryption** process method requires a public **key** , a common key, etc. of each other between the source and the destination (receiver) of data, a complicated process should be performed including user authentication. Furthermore, **encrypted data** cannot be transmitted between the source and the destination unless the encryption interfaces including the...

...payer and payee are subject to a risk of returning goods.

In transactions through a **network** , both payer and payee are subject to various risks such as an illegal use risk...

...providing a settlement system capable of safely trading in goods (or a commodity) through a **network** or without a **network** (offline) with the above described various risks removed using a payment means such as electronic...

...can solve the problem of a collection risk. When a transaction is processed through a **network** ., a payee can easily authenticate a payer by issuing a request for final settlement of...

...for mediating data from the first party to the second party, has a unit for **encrypting data** using a unique **encryption key** between the first party and the transaction management device and issuing a request to the...

...the encryption intermediate system and the first and second parties who transmit and receive encrypted **data** manage unique encryption and decryption **keys** . A transmitter transmits **encrypted data** with a transmission request specifying a destination without caring about an encryption interface with the...

...unique decryption key shared between the transmitter and the transaction management device, and then re- **encrypts** using the unique **encryption key** shared between the specified destination and the transaction management device the **data** into **encrypted data** which can be decrypted by the destination only. The receiver receives the **encrypted data** from the transaction management device, and decrypts the data using the unique decryption key shared...

...device and the receiver without caring about the encryption interface with the source of the **encrypted data** . Therefore, there is no risk that the third party may decrypt the data.

That is, since the transmitter transmits **data encrypted** using a unique **encryption key** shared between the transaction management device and the transmitter without caring about an **encryption key** or a decryption **key** shared between the transmitter and the destination, the transmitter need not transmit or receive any **encryption** or decryption **keys** to or from any receiver. Therefore, it is easy on both transmitting and receiving sides to manage an **encryption key** and a decryption **key** , and no attention should be paid to an encryption method, an encryption application interface, etc...

...party and the second party in the data transmission, and includes a unit for receiving **data** using a unique **encryption** protocol between the first party and the transaction management device; and a unit for transmitting the received **data** using a unique **encryption** protocol between the transaction management device and the second party.

With the above described configuration...

...device. Therefore, a transmitter of transaction information need not request to receive a receiver's **encryption key** or send its own **encryption key** . Additionally, since the transmitter transmits **data encrypted** using a unique **encryption key** shared between the transaction management device and the transmitter, the transmitter need not transmit or receive any **encryption** or decryption **keys** to or from any receiver. Therefore, there is no risk that the third party may decrypt the transaction information. Furthermore, it is easy for the transmitter to manage an **encryption key** , and no attention should be paid to an encryption method, an encryption application interface, etc...

appropriate combination with other **encryption** **keys** /decryption **keys** . For example, a transmitter (A or TC) can encrypt an electronic message using a transmitter...

...C, A) or K(C,TC), and transmit the encrypted message together with a common **key** **encrypted** using the unique public **key** K(P(TC), (gamma)) (where (gamma) is A or B, C) between the transmitter and the receiver (TC or B, C). In this case, the receiver decrypts the **encrypted** common **key** using a secret **key** , and decrypts the electronic message using the decrypted common **key** .

To furthermore improve the **security** of the electronic message, the transmitter 1200 (A) can also execute a digital signature as...

...s secret key K(S,A), assign a blind signature using the transmitter's common **key** K(C,A), and **encrypt** the entire message using the only and unique **encryption** **key** K(C(A), TC) or K(P(TC), A) between the transmitter and the transaction...and a return-of-goods site monitor process 2500.

In the data transmission/receipt, the **encryption** /decryption process 1520 decrypts **data** **encrypted** by a transmitter when it receives the **data** , and transmits the **data** after **encrypting** it using an **encryption** **key** exclusively used for a receiver. This process is a common process used in the other...

...and from each device. If it receives data in step 1522, the transmitter-exclusive decryption **key** 1120 is retrieved from the **encryption** **key** management DB 50 in the transaction management device 5 as described above in step 1524. In step 1526, the **data** **encrypted** using the transmitter-exclusive **encryption** **key** is decrypted using the retrieved key.

When data is transmitted after a predetermined process is...

...information management DB such as the seller information DB 52, and the transmitter-exclusive encryption **key** 1120 is retrieved from the **encryption** **key** management DB 50 in step 1532. In step 1534, the transmission **data** is encrypted using the encryption **key** 1120. In step 1536, the **encrypted** **data** is transmitted according to the receiver information.

When a transaction is mediated between two devices...

...transmitter's encrypted electronic message is decrypted in the above described procedure, and then re- **encrypted** using the receiver's **encryption** **key** for transmission as shown in FIG. 24.

In the process flow in the transaction management...

...digital contents in the above described process, the transaction management device 5 manages the decryption **key** of the digital contents **encrypted** by the seller and transmitted to the purchaser, transmits the decryption key to the purchaser...

...term 1373 of the return-of-goods management information 1370 are set in the state **before** transmission of the **decryption** **key** , and the final settlement site monitor DB 56 is deleted. In step 2192, since it...
address, telephone number, etc.) 4412, transmission/receipt management information (address, ID, etc.) 4414, and authentication **information** (**encryption** **key** , etc.) 4416.

Each of the processes of the delivery management process unit 4480 is described...request, and points to a record of the final settlement request management DB 7400. An **encryption** **key** 7216 and a decryption **key** 7217 of digital contents key information are information used when digital contents are sold.

FIGs...

...for linking to the goods management DB 7100, a digital contents classification code 7552, digest **information** 7553, **encryption** identification type 7554, and contents goods **information** 7555. The **encryption** identification type 7554 specifies an encryption/decryption system of digital contents. The digital contents are...

...to FIG. 86. In step 7702, the digital contents transmission process 7700 transmits the digest **information** about digital contents and **encrypted** digital contents.

The digital contents transmission process 7700 refers to the digital contents management DB...

...retrieves the digest information 7553 of the corresponding digital contents record. Furthermore, the contents goods **information** 7555 is **encrypted** using the **encryption** **key** 7216 of the digital contents key information of the sales management DB 7200. These data...

...request is issued in step 7914, then non-encrypted digital contents are re-transmitted after **encrypting** them using an **encryption** **key** between the seller's processing unit 2 and the transaction management device 5 in step...output device 8104, an external storage device 8105, a media drive device 8106, and a **network** connection device 8107. These components are interconnected through a bus 8108.

The memory 8102 stores...

...portable storage medium 8109, and loaded onto the memory 8102 for use as necessary.

The **network** connection device 8107 communicates with other devices through an optional **network** (line) such as a LAN (local area **network**), etc., and converts data for communications. When it is necessary, the above described program and...

...provisional settlement information for other uses.

According to the present invention, since the payment object **information** is **encrypted** (blinded) using an **encryption** **key** so that only the issuing financial institution can decrypt the information, the money information can...

...medium such as a portable card, etc., a payer can transmit payment to a payee **online** through a **network** , etc. when purchasing goods, or can pay by directly providing the portable storage medium. As...

...settlement request. Therefore, even a payee not provided with a processing unit connected through a **network** can process a transaction using the provisional settlement system.

According to the present invention, when...

...to the payee's financial institution containing the payee's account, or the payee's **electronic** **wallet** information. Thus, when the final settlement is made, the transfer is automatically executed to the...

...processed through an intermediate for transmission (transaction management device, etc.). Therefore, a transmitter of transaction **information** need not receive an **encryption key** of a receiver or send the transmitter's **encryption key** . Since the transmitter transmits a message after **encrypting** it using a unique **encryption key** between a transmission intermediate and the transmitter, the transmitter need not transmit or receive an **encryption key** or a decryption **key** to or from the receiver. Therefore, there is no risk that a third party may read the transaction information. Furthermore, the transmitter can easily manage the **encryption key** , thereby largely improving the **security** .

Furthermore, according to the present invention, a transmission intermediate decrypts an encrypted electronic message transmitted...

...authenticating the transmitter.

According to the present invention, since a receiver receives an electronic message **encrypted** using a unique **encryption key** between the intermediate and the receiver, the receiver need not consider the **encryption key** of the transmitter. Additionally, the receiver can easily manage the **encryption key** , thereby largely improving the **security** .

Furthermore, according to the present invention, since transaction conditions cannot be confirmed if a transaction...

The Applicant Itself

```
 51/3,K/19     (Item 19 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2006 European Patent Office. All rts. reserv.

01258375
SYSTEM  AND  METHODS  FOR  MAINTAINING  AND  DISTRIBUTING PERSONAL SECURITY
    DEVICES
SYSTEM   UND  VEFAHREN  ZUR  ERHALTUNG  UND  VERTEILUNG  VON  INDIVIDUELLEN

    SICHERUNGSEINRICHTUNGEN
SYSTEME   ET   PROCEDE  DE  MAINTENANCE   ET DE DISTRIBUTION DE DISPOSITIFS DE
    SECURITE PERSONNELS
PATENT ASSIGNEE:
  RSA Security Inc., (811596), 36 Crosby Drive, Bedford, MA 01730, (US),
    (Applicant designated States: all)
INVENTOR:
   DUANE ,  William , 4 Howard Road, Westford, MA 01886, (US)
   ROSTIN ,  Peter , Gardsmygvagen 6, S-135 68 Tyreso, (SE
LEGAL REPRESENTATIVE:
  Simons, Alison Diane et al (95571), Dummett Copp 25 The Square Martlesham
    Heath, Ipswich, Suffolk IP5 3SL, (GB)
PATENT (CC, No, Kind, Date):  EP 1201070  A2  020502 (Basic)
                              WO 200106699  010125
APPLICATION (CC, No, Date):   EP 2000948778 000719;  WO 2000US19656  000719
PRIORITY (CC, No, Date): US 356600 990719
DESIGNATED STATES: DE; FI; FR; GB; IE; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7):  H04L-029/06
NOTE:
  No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English

INVENTOR:
   DUANE ,  William , ...

...US)
   ROSTIN ,  Peter ,
INTERNATIONAL PATENT CLASS (V7):  H04L-029/06
```

51/3,K/23 (Item 23 from file: 349)

00368338
SYSTEM AND METHOD FOR COMMERCIAL PAYMENTS USING TRUSTED AGENTS
SYSTEME ET METHODE DE PAIEMENTS COMMERCIAUX FAISANT APPEL A DES "AGENTS DE CONFIANCE"

Patent Applicant/Assignee:
CITIBANK N A,
Inventor(s):
ROSEN Sholom S,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9708665 A1 19970306
Application: WO 96US3824 19960322 (PCT/WO US9603824)
Priority Application: US 95521262 19950830
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IS JP KE
KG KP KR KZ LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE
SG SI SK TJ TM TR TT UA UG UZ VN KE LS MW SD SZ UG AM AZ BY KG KZ MD RU
TJ TM AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI
CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 11836

International Patent Class (v7): **G06F-17:60**
Fulltext Availability:
Detailed Description
Claims

Detailed Description
... payments between money modules (e.g. , between a money module contained within a customer's " **electronic wallet** " and a money module contained within a merchant's point-of-sale terminal), or on-line payments for **network** services such as information retrieval and telephone calls, or for purchasing airline tickets, theater tickets...5D illustrate the functional components of trusted agents,
Figure 6 is a diagram showing the **network** structure for commercial money module payment.

Figure 7A illustrates a Commit protocol.

Figure 7B illustrates...
...trusted agent is a combination,of hardware and software components. It is tamper-proof and **contains secure** protocols which cooperate with a money module to synchronize secure payment to delivery. Money modules...

...07/794,112 and 08/427,287.

The trusted agents when making purchases over a **network** , exchange electronic merchandise and payment. In the present invention for making commercial payments, as shown...

...customer trusted device.

The remittance advice is sent to the trusted device over the customer **network** . As shown in Figure 2A, the remittance advice contains information needed to consummate the transactions...

...the name and address of the customer and merchant, a customer reference number, and the **network** address of the merchant, the amount to be paid 49, the date of payment 48...and described, for example, in D.W.

Davies and W.L. Price, Security For Computer **Networks** (John Wiley & Sons, 1984).

The Transfer History section 18 contains --information generated when tickets are...

...Times field 34 contains the date and time of transfer of the ticket 8. As **subsequent** transfers are made, additional receiver and sender ID's, sender **certificates** , and dates and times are appended to each field, thus creating a list of transfer...

...up the connection between two transaction devices 122, or connects a transaction device to a **network** for indirect connection to another transaction device or a trusted server.

Transaction Applications 130 may...Manager function 142 sets up and breaks
down inter-agent sessions and agent to trusted **server** sessions. A **Security** Manager function 144 maintains **security** **information** (e.g., a trusted agent certificate and an untrusted agent list) and establishes secure communication...random source f or a random number generator.

System Overview
Figure 6 shows the general **network** architecture of the contemplated system for commercial payments. Customer transaction device 188 can communicate with the customer's accounts payable system 189 via the customer **network** 191.

The customer's accounts payable system creates the remittance advice having a list of...has both the remittance advice and the electronic money, it can connect with a merchant **network** 134 over some gateway **network** 190. The merchant **network** provides communications for MTD 198 and the merchant's accounts receivable system 193. The accounts...the HTA) HTA then connects to host transaction application B (HTB) preferably via a customer **network** 191, gateway **network** 190 and merchant **network** 134 (step 700), and the customer

chooses to make a commercial payment. HTA sends...verification message,

and cert(TA) into a message for trusted agent A (step 320). Public **Key** B
- 19
encrypts the message using trusted agent A' s public key (TA (PK)) which trusted agent B...TA/TA) by exclusive ORing random numbers R(A) and R(B) (step 344). Session **key** (TA/TA) is used to **encrypt** communications between two trusted agents 120. Session Manager A assembles a message containing the A and B verification messages, the date/time information, and R(A) (step 344). Public **Key** A **encrypts** the message with trusted server B's public key (received by A in cert(TAH...

...Public Key B decrypts the received message using its secret key (corresponding to its public **key**) (step 352).

Security Manager B checks if the B verification message received from A is the same B...

...is the same, then Session Manager B notes the start of the session (step 358).
Security Manager B forms session **key** (TA/TA) by R(A) XOR R(B) and then stores the session key (step...

...used for their current interaction. Next, Date/Time B sends its current date and time **information** to **Security** Manager B (step 362).

Security Manager B assembles a message having an acknowledgement to A...

...the message from B to A.

Referring to Figure 10, trusted agent B's Symmetric **Key** function **encrypts** the message using session -- **key** (TA/TA) (step 376). Message Interface B then formats the message and sends it to...

...strips out the message (steps 382 384). Symmetric Key A decrypts the message with session **key** (TA/TA) thus completing the **secure** communication of a message between trusted agent and trusted agent using session key (TA/TA...

...Manager A receives the acknowledgement, A verif ication message and B I s date/time **information** (step 368). **Security** Manager A checks if the A verification message is the same A verification message which...established during a transaction.

Encryption channel 436 between the two trusted agents 120 carries messages **encrypted** by session **key** (TA/TA) . Channels 438 and 440 between a trusted agent 120 and its money module...

...between money modules 6 in different transaction devices 122 use session key (MM/MM).

Session **key** (TA/W is used for **encrypting**
messages sent between a trusted agent 120 and its associated
money module 6 via encryption...messages via the pre-existing trusted
agent's
session.

Claim

... trusted agent and said merchant trusted agent;

(b) said customer trusted agent transferring remittance advice **information** , via said first cryptographically **secure** session, to said merchant trusted agent;

(c) said merchant trusted agent creating a commercial payment advice information over a communication **network** , comprising:

a tamper-proof first electronic agent having a first processor;

a tamper-proof first...

...that established a first cryptographically secure session with said first electronic agent over said communication **network** , and having a third processor;

a tamper-proof second money module associated with and that...

...having a fourth processor;

where said f irst processor is adapted to transfer remittance advice **information** , via said first cryptographically **secure** session, to said second electronic agent;

where said third processor creates a commercial payment ticket...

...said list are summed and compared to a total amount included in said remittance advice **information** .

12 A system for **securely** linking electronic commercial payment to remittance advice information, comprising:

a tamper-proof first electronic transaction...

51/3,K/28 (Item 28 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01957307
Trusted infrastructure support systems, methods and techniques for secure electronic commerce and rights management.
Vertrauenswurdige Infrastrukturbetreuungssysteme, Verfahren und Techniken zum sicheren elektronischen Handel zur Rechtverwaltung
Systemes de support d'infrastructure de confiance, methodes et techniques pour le commerce electronique securise et la gestion de droits

PATENT ASSIGNEE:
Intertrust Technologies Corp., (2434320), 460 Oakmead Parkway, Sunnyvale, CA 94086-4708, (US), (Applicant designated States: all)

INVENTOR:
Shear, Victor H., 5203 Battery Lane, Bethesda MD 20814, (US)
Van Wie, David M., 1780 East 25th Avenue, Eugene OR 97403, (US)
Weber, Robert P., 215 Waverly Street nr.4, Menlo Park CA 94025, (US)

LEGAL REPRESENTATIVE:
Smith, Norman Ian et al (36041), fJ CLEVELAND 40-43 Chancery Lane, London WC2A 1JQ, (GB)

PATENT (CC, No, Kind, Date): EP 1577816 A2 050921 (Basic)
APPLICATION (CC, No, Date): EP 2005076225 960904;
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
RELATED PARENT NUMBER(S) - PN (AN):
EP 974129 (EP 96932173)
INTERNATIONAL PATENT CLASS (V7): **G06F-017/60** ; G07F-019/00
ABSTRACT WORD COUNT: 252
NOTE:
Figure number on first page: 4

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200538	1074
SPEC A	(English)	200538	66190
Total word count - document A			67264
Total word count - document B			0
Total word count - documents A + B			67264

INTERNATIONAL PATENT CLASS (V7): **G06F-017/60** ...

...ABSTRACT usage clearing, secure directory services, and other transaction related capabilities functioning over a vast electronic **network** such as the **Internet** and/or over organization internal Intranets. These administrative and support services can be adapted to...

...reuse these services in response to competitive business realities. A Distributed Commerce Utility having a **secure** , **programmable** , distributed architecture provides administrative and support services. The Distributed Commerce Utility makes optimally efficient use...

...of its participants. Different support functions can be collected together in hierarchical and/or in **networked** relationships to suit various business models and/or other objective. Modular support functions can be...

...SPECIFICATION the Inventions

These inventions generally relate to optimally bringing the efficiencies of modem computing and **networking** to the administration and support of electronic interactions and consequences and further relate to a...

...administration, electronic process control and automation, and clearing functions across and/or within an electronic **network** and/or virtual distribution environment; and/or

* clearing, control, automation, and other administrative, infrastructure and support capabilities that collectively enable and support the operation of an efficient, **secure** , peer-to-peer collection of commerce participants within the human digital community.

Background

Efficient, effective...

...it possible and efficient, and allow the wheels of commerce to spin smoothly.

Suppose you **want** to buy bread at the local bakery. The baker doesn't have to do everything...

...services.

More and more of the world's commerce is being carried on electronically. The **Internet** -- a massive electronic **network** of **networks** that connects millions of computers worldwide -- is being used increasingly as the vehicle for commerce...

...initiate purchase and then to complete a simple form to convey credit card information), the **Internet** is rapidly becoming a focal point for consumer and business to business purchases. It is...

...games, and entertainment.

At the same time, large companies use both private and public data **networks** to connect with their suppliers and customers. Driven by apparently inexorable declines in the cost of both computing power and **network** capacity, electronic commerce will increase in importance as the world becomes more and more computerized...

...relationships. Electronic commerce on any significant scale will require a dependable, efficient, scaleable, and secure **network** of third party support and administrative service providers and mechanisms to facilitate important parts of...

...structures and arrangements that enable secure, efficient distributed electronic commerce and rights management on the **Internet** (and Intranets), within companies large and small, in the living room, and in the home...

...electronic rights management.

The Ginter, et al. patent specification also describes an "Information Utility" - a **network** of support and administrative services, facilities and installations that grease the wheels of electronic commerce...

...usage clearing, secure directory services, and other transaction related capabilities functioning over a vast electronic **network** such as the **Internet** and/or over organization internal Intranets, or even in-home **networks** of electronic appliances.

These administrative and support services can be adapted to the specific needs...

...response to competitive business realities.

The present inventions provide a "Distributed Commerce Utility" having a **secure** , **programmable** , distributed architecture that provides administrative and support services. The Distributed Commerce Utility can make optimally...

...of its participants.

Different support functions can be collected together in hierarchical and/or in **networked** relationships to suit various business models and/or other objectives. Modular support functions can be...

...of human electronic interaction and relationships.

* Optimally applies the efficiencies of modem distributed computing and **networking** .
* Provides electronic automation and distributed processing.
* Supports electronic commerce and communications infrastructure that is modular, **programmable** , distributed and optimally computerized.
* Provides a comprehensive array of capabilities that can be combined to ...

...and distributed processing to produce optimal allocation and use of resources across a system or **network** .
* Is efficient, flexible, cost effective, configurable, reusable, modifiable, and generalizable.
* Can economically reflect users' business...

...as a mixture of distributed and centralized processes.
* Provides a blend of local, centralized and **networked** capabilities that can be uniquely shaped and reshaped to meet changing conditions.
* Supports general purpose...

...requirements.
* Can support any number of commerce and communications models.
* Efficiently applies local, centralized and **networked** resources to match each value chain's requirements.
* Sharing of common resources spreads out costs and maximizes efficiency.

* Supports mixed, distributed, peer-to-peer and centralized **networked** capabilities.
* Can operate locally, remotely and/or centrally.
* Can operate synchronously, asynchronously, or support both...

...overlay necessary for realizing maximum benefits from electronic automation, distributed processing, and system (e.g., **network**) wide optimal resource utilization.
* The Distributed Commerce Utility is particularly adapted to provide the administrative foundation for the **Internet** , organization Intranets, and similar environments involving distributed digital information creators, users, and service systems.
* The...

...can be uniquely shaped and reshaped to progressively reflect optimal blends of local, centralized, and **networked** Distributed Commerce Utility administrative capabilities.
* The Distributed Commerce Utility's innovative electronic administrative capabilities support mixed, distributed, peer-to-peer and centralized

networked capabilities. Collections of these capabilities, can each operate in any mixture of local, remote, and central asynchronous and/or synchronous **networked** combinations that together comprise the most commercially implementable, economic, and marketable - that is commercially desirable...

...of commerce and communication models which share (e.g., reuse), as appropriate, local, centralized, and **networked** resources. As a result, the Distributed Commerce Utility optimally enables practical and efficient electronic commerce...

...processing environments" disclosed in Ginter et al.
* Distributed clearinghouse operations may be performed through "virtually **networked** and/or hierarchical" arrays of Commerce Utility System sites employing a general purpose, interoperable (e...

...sites.
* One or more parts of the Distributed Commerce Utility may be comprised of a **network** of distributed protected processing environments performing one or more roles having hierarchical and/or peer...

...as the number of VDE participant protected processing environments and/or may have specific hierarchical, **networked** and/or centralized administration and support relationship(s) to such participant protected processing environments.
* In...

...centralized service protected processing environments.
* The Distributed Commerce Utility is especially useful to support the **Internet** and other electronic environments that have distributed information creators, users and service providers. By helping...

...plays a fundamentally important role in migration of these non-electronic human activities onto the **Internet** , Intranets, and other electronic interaction **networks** . Such **network** users require the Distributed Commerce Utility foundation and support services in order to economically realize their business and privacy requirements. This **secure** distributed processing foundation is needed to optimally support the capacity of electronic commerce models to...
...of their operation.
* The Distributed Commerce Utility can ensure appropriately high levels of physical, computer, **network** , process and policy-based security and automation while providing enhanced, efficient, reliable, easy to use...
F. fingerprinting,
* G. other VDE security techniques,
* H. rights operating system,
* I. object design and **secure** **container** techniques,
* J. **container** control structures,
* K. rights and process control language,
* L. electronic negotiation,
* M. secure hardware, and...

...can be combined in various ways and/or distributed through an electronic community, system or **network** . The preferred embodiment uses the protected processing environment based Virtual Distribution Environment described in Ginter...

...might be distributed in and/or throughout existing or new communications infrastructure or other electronic **network** support components.
* Other support services might operate within secure execution spaces (e.g., protected processing...
...a secure web of support service fabric.
* Other support services might operate both in the **network** support infrastructure and at user electronic appliances.
Such distributed support services may complement (and/or....

...subsequently adapt (modify), any support service functions to any desired degree across a system or **network** provides great power, flexibility and increases in efficiency. For example, distributing aspects of support services...

...may provide administrative support for any or all of the following:
* trusted electronic event management,
* **networked** , automated, distributed, secure process administration and control,
* Virtual Distribution Environment chain-of-handling and control...

...g., event) management (e.g., auditing, control, rights fulfillment, etc.)

.), across and/or within electronic **networks** , including "unconnected," virtually connected, or periodically connected **networks** .
The Commerce Utility Systems may govern electronic process chains and electronic event consequences related to...
...activities,
* compiling, aggregating, using and/or providing information relating to use of one or more **secure** **containers** and/or content and/or processes (events), including contents of **secure** **containers** and/or any other content,
* providing information based upon usage auditing, user profiling, and/or market surveying related to use of one or more **secure** **containers** and/or content and/or processes (events),
* employing information derived from user exposure to content...

...discount buyers club membership);
* third party archiving and/or authenticating of transactions and/or transaction **information** for **secure** backup and non-repudiation,
* providing **programmed** mixed arrays of Commerce Utility System process control and automation services, where different Commerce Utility...

...or business models requirements, and where such Commerce Utility Systems further support distributed, scaleable, efficient **networked** and/or hierarchical fixed and/or virtual clearinghouse models which employ secure communication among a...

...consumer appliance 100 electronically connected to Distributed Commerce Utility 75. In this example, an electronic **network** 150 connects appliance 100 to Distributed Commerce Utility 75. Distributed Commerce Utility 75 supports the...

...receive television programs from television broadcasters 110 and/or satellites 112 via a cable television **network** 114, for example. Player/recorder 104 could play various types of program material from tapes...

...may be based on one or more computer chips, such as a hardware and/or **software** based " **secure** processing unit" as shown in Figure 9 of the Ginter et al. Patent specification. The...

...may insist upon the protected processing environment 154 providing a copy protection mechanism 120 that **securely** protects against copying video **program** 102a. Distributed Commerce Utility 75 may include a special purpose Commerce Utility System 90c called...

...assist the protected processing environment 154 in communicating electronically with other computers and appliances over **network** 150;
* A "transaction authority" 700 that may be available for process control and automation such...
...addition, some of the functions of the Commerce Utility System 90 may be distributed within **network** 150 - for example, in the ...other administrative and support service functions (for example, issuance of important digital certificates, maintaining massive **data** bases supporting **secure** directory services, etc.) are much more centralized. The degree of distributedness of any particular administrative...

...comprise a vast "web" of distributed, partly distributed and/or centralized Commerce Utility Systems 90. **Network** 150 can be used to connect this web of Commerce Utility Systems 90 to a...

...200B -- both of which are located in Japan on the company's internal, private corporate **network** (or Intranet) 1072. From time to time and in accordance with VDE controls associated with...
...with VDE rules and controls managing protected processing environment processes and sends in a VDE **secure container** the audit records 302(3) to the external, commercial usage clearinghouse 300. All of the company's internal, distributed usage clearinghouses 300A, 300B, 300C send periodic communications in VDE **secure containers** 152 to the commercial usage clearinghouse 300. In turn, the master usage clearinghouse 300 creates...

...The internal, distributed financial clearinghouses 200A, 200B, 200C also receive audit records 302 in VDE **secure containers** 152 in accordance with VDE controls sets for the purchased information from each of the...

...clearinghouse 200A, 200B, 200C aggregates the payments and from time to time sends a VDE **secure container** 152 with audit records 302 indicating the aggregate sums to be transferred to the information...

...appliances 1074 report their usage and financial transactions to headquarters-based clearinghouses 200HQ, 300HQ in **secure containers** 152 over Intranet 1072. Company headquarters financial clearinghouse 200HQ may interface directly into VDE compliant...

...organization A (left-hand side of the drawing) as having an "Intranet" (a private data **network** within a particular organization) 5100(A). Intranet 5100(A) may be a local and/or wide area **network** for example. User electronic appliances 100(A)(1),..., 100(A)(N) (for example, employees of...

...N), and private transaction authority 700(B). In addition, Figure 66 shows a public data **network** 5104 (such as the **Internet** for example) and a public transaction authority 700(C). Figure 66 shows that in this ...

...authority 700(A), 700(B) need not be the actual "gateway" and "firewall" to/from **Internet** 5104, but could instead operate wholly internally to the respective organizations A, B while potentially generating electronic containers 302 for transmission over **Internet** 5104.

In this example, organization A user protected processing environments 100(A)(1),..., 100(A...

...environment protected processing environment, and can communicate with one another over Intranet 5100(A) via **secure** electronic **containers** 302. Similarly, organization A user electronic appliances 100(B)(1),..., 100(B)(N) each have...
...environment protected processing environment, and can communicate with one another over Intranet 5100(B) via **secure** electronic **containers** 302. In addition, organization A and organization B can communicate with one another over **Internet** 5104 via **secure** electronic **containers** 302.

Organization A's private trusted transaction authority 700(A) may be used for facilitating...

...CLAIMS comprising:
a first electronic appliance (100),
a second electronic appliance (100'), and

an electronic communications **network** (150) that allows the first and second electronic appliances (100, 100') to exchange digital signals ...

...to at least one of the first and second electronic appliances (100, 100') through the **network** (150), the third electronic appliance performing a third part of the clearing operation.

12. An...

...or rights management system according to any preceding claim, further characterised in that the electronic **network** (150) couples the first and second electronic appliances (100, 100') to a commerce utility system.·..

...management system according to any preceding claim, further characterised in that that clearing operation includes **securely** providing directory **information** .

27. An electronic commerce and/or rights management system according to any preceding claim, further...

```
 51/3,K/29     (Item 29 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2006 European Patent Office. All rts. reserv.

01297342
DEALING METHOD AND DEALING SYSTEM
TRANSAKTIONS-VERFAHREN UND TRANSAKTIONS-SYSTEM
PROCEDE DE TRANSACTION ET SYSTEME DE TRANSACTION
PATENT ASSIGNEE:
  FUJITSU LIMITED, (211463), 1-1, Kamikodanaka 4-chome, Nakahara-ku,
    Kawasaki-shi, Kanagawa 211-8588, (JP), (Applicant designated States:
    all)
INVENTOR:
  HOSHINO, Masao Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku,
    Kawasaki-shi, Kanagawa 211-8588, (JP)
  NISHIO, Nobuhiko Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku,
    Kawasaki-shi, Kanagawa 211-8588, (JP)
LEGAL REPRESENTATIVE:
  Kreutzer, Ulrich, Dipl.-Phys. (90474), Cabinet Beau de Lomenie,
    Bavariaring 26, 80336 Munchen, (DE)
PATENT (CC, No, Kind, Date):  EP 1225533  A1  020724 (Basic)
                              WO 200131548  010503
APPLICATION (CC, No, Date):   EP 99947858 991007;  WO 99JP5563  991007
DESIGNATED STATES: FR
INTERNATIONAL PATENT CLASS (V7):  G06F-019/00 ;  G06F-017/60
ABSTRACT WORD COUNT: 126

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:
Available Text  Language   Update    Word Count
      CLAIMS A  (English)  200230      480
      SPEC A    (English)  200230    26159
Total word count - document A        26639
Total word count - document B            0
Total word count - documents A + B   26639

INTERNATIONAL PATENT CLASS (V7):  G06F-019/00 ...

... G06F-017/60

...SPECIFICATION card.

  BACKGROUND TECHNOLOGY
    Recently electronic commerce using an IC card, which is referred to as
  electronic  wallet  transaction, becomes in practical use. This
  electronic  wallet  transaction system is such a system that cash data
  corresponding to money is provided in...
...s IC card and it is transferred to the transaction equipment. The IC
  card for electronic  wallet  transaction is constituted by a one-chip
  microcomputer including a nonvolatile RAM and a processor...

...of money as the electronic value and a personal identification number
  (PIN) are stored. Further, program  modules for  encryption /decryption
  processing are stored in this nonvolatile RAM. Also, using these program
  modules, an authentication...

...to a magnetic card being vulnerable to falsification or illegal readout
```

of recorded data.
The **electronic wallet** transaction is a method in which a traditional procedure of cash payment out of a...

...balance maintained in the memory of the transaction equipment increases for that amount.
In such **electronic wallet** transaction, it is not necessary to prepare cash for shopping or the like, thereby reducing...

...in the official gazette of Japanese Unexamined Patent Publication No. Hei-9-161152)
To promote **electronic wallet** transaction using an IC card, a combined method of the **electronic wallet** transaction and a customer service system may be considered. As an example, there has been proposed, in the official gazette of Japanese Unexamined Patent Publication No. Hei-7-334590, an **electronic wallet** transaction system combined with a point card service of a coupon ticket.
In such a system, there can be initiated to perform a service in connection with an **electronic wallet** transaction. However, when such a service is carried out, procedures for collecting, totaling and settling...

...management equipment and IC card therefor, enabling to provide customer services so as to promote **electronic wallet** transactions.
It is still another object of the present invention to provide transaction method, transaction...

...customer services with high security when such customer services are provided in the course of **electronic wallet** transactions.

DISCLOSURE OF THE INVENTION
According to one feature of a transaction method in the...transaction data. Also, using an IC card, it is not necessary to install a particular **online network** . Further, because the management equipment reads out transaction data from the IC card being provided...

...equipment includes a card reader/writer for exchanging information with a customer IC card having **electronic wallet** transaction function; a card reader/writer for exchanging information with the IC card; and a processing unit for performing an **electronic wallet** transaction by transferring **electronic** value in the customer IC card to the IC card.
Accordingly, as the service transaction is added to the **electronic wallet** transaction, the service transaction convenient for customers can be given to the **electronic wallet** transaction.
According to another feature of the transaction method in the present invention, the storage...

...of the transaction system in the present invention, the transaction equipment issues service information on **electronic wallet** transaction.
According to further feature of the transaction system in of the present invention, the transaction equipment reflects a service being performed according to the extracted service information to the **electronic wallet** transaction.
Through these embodiments, customer services directly reflecting to **electronic wallet** transaction can be achieved.
According to one embodiment of management equipment of the present

invention...an IC card of the present invention, the IC card includes a memory having an **electronic wallet** area and a service information storage area for storing service information of the service having been provided to a customer. Because the IC card has both **electronic wallet** transaction function' and service ticket transfer function, it is easily possible to add a service function to the IC card having **electronic wallet** transaction function.

According to another embodiment of the IC card of the present invention, a processor stores into the aforementioned memory the service information including a service ticket identification **data** and an **encrypted** signature generated based on the above identification **data** . Storing the **encrypted** signature enables to provide security against illegalities.

According to another embodiment of the IC card...

...PRESENT INVENTION

Hereinafter the present invention is explained in order of transaction system, IC card, **electronic wallet** transaction equipment, and management equipment.

(center dot) (center dot) IC card transaction system (center dot customer IC card 2 has an **electronic wallet** area, a service ticket area, an advertising area, and an electronic signature area.

A POS terminal 1 configures **electronic wallet** transaction equipment that performs the **electronic wallet** transaction by operating with the customer IC card 2. Here, an **electronic wallet** is defined as a wallet that possesses cash in the form of **electronic** value. Here **electronic wallet** transaction is basically a transaction that performs to transfer the electronic value. In addition, the **electronic wallet** transaction includes a transaction in which electronic value is transferred in secrecy using **encryption** and decryption functions and the **information** related to the value to be transferred is protected from forgery or other illegality using...

...terminal 1 is provided with a service ticket processing function 5 in addition to the **electronic wallet** transaction function. The service ticket processing function 5 performs functions of issuing and collecting service...

...service tickets which are subjects of transfer from one side of an IC card or **electronic wallet** transaction equipment, to the opposite side. After this transfer, the electronic cash or service tickets...
...which is arbitrarily set. In such a case, the POS terminal 1 issuing a lot **encrypts** the lot using a **key** number that becomes a key of interest. Further, winning lot confirmation equipment has a key number table storing a key number corresponding to the shop number and read the **key** number from the table. Thus **encryption** and decryption are carried out. Otherwise, a lot number to be shown to a customer...as well as a digital signature thereto is written into the IC card 2, when **electronic wallet** transaction using the IC card 2 is carried out. The lot is configured so that...

...trouble-some, enabling easy data handling.

This store IC card 3 is provided with the **electronic wallet** transaction function. Therefore it is also possible to use the store IC card 3 as...

...decreased manual intervention improves reliability. This method can be implemented without configuring a large-scale **online network** .

Connection unit 7 transfers electronic money and service tickets stored in the customer IC card...card 3 is performed via this bus line 23. Therefore, it is possible to improve **security** of the transfer **data** .

As for processing function of the controller 17, there are provided functions of **electronic wallet** transaction by means of the customer IC card 2, commission of issuing service tickets, commission...payment, i.e. whether the payment is to be made by cash, credit card, or **electronic wallet** using the IC card. Depending on this inquiry result, the shop clerk operates the keyboard...

...or credit card, or step S207 namely a processing routine for the payment by the **electronic wallet** .

(S204) In case the payment by cash or credit card is specified, the controller 17...

...POS terminal falls into a transaction waiting state.

(S207) Meanwhile, in case the payment by **electronic wallet** is specified as the payment type, the controller 17 reads from the customer IC card...receipt.

(S212) Then, the controller 17 calculates a transaction amount to be withdrawn from the **electronic wallet** of customer IC card 2. This calculation result is obtained by subtracting the discount value...

...store IC card 3 through the store IC card reader/writer 21 to perform an **electronic wallet** transaction of this transaction amount.

As further explained in FIG. 9, based on the aforementioned...

...a transaction amount of the requested transfer together with the information indicating the completion of **electronic wallet** transaction, and the printer 14 prints out it onto the receipt. For example, "Electronic money...

...12345" is printed out on the receipt. Thus the commission-processing step S212 of the **electronic wallet** transaction is completed.

(S213) Then, the controller 17 requests the store IC card 3 to... totaled to print out. The processing is then completed.

In such a manner, when the **electronic wallet** transaction is performed by the POS terminal 1, the store IC card 3 of the...

...lot, betting ticket and coupon ticket to the customer IC card 2 used as an **electronic wallet** , and of extracting and collecting such a service ticket. The service information can be transferred...

...tickets enable to reduce a lord work on a shop side.

In relation to the **electronic wallet** transaction, services such as discounting can be performed. Therefore, an attraction of the **electronic wallet** transaction is improved to the customers. This also benefits the shops introducing cards for attracting...

...the memory 35 a directory 40 and an OS program 41, as well as an **electronic wallet** area 42, a lottery and betting ticket information area 43, a coupon ticket area 44 are stored an access right table 46, a personal identification number (PIN) 47, an **encryption key** 48 for use in the authentication program, and a variety of application programs 49.

In the **electronic wallet** area 42, a remainder of electronic money and an electronic signature therefor are stored. Further...

...transaction and are stored in the area 42. Tens of transactions can be recorded in **electronic wallet** area 42, each partitioned area is controlled so as to use cyclically in a known...

...the access right information in the access right table.

For example, in FIG. 6, accessing **electronic wallet** data stored in the **electronic wallet** area 42 as shown in Fig.5 is permitted to read when the access is...

...such as writing, deletion and update are inhibited for these access equipments. In regard to **electronic wallet** data, lottery/betting information, and coupon information, the access right thereto is preset so that...

...in FIG. 6; a personal identification number 705 of the owner of the IC card; **key information** (encryption **key**) 706 for use in **encrypting** transmission **information** ; and an application area 707 for storing a variety of application programs.

As areas in a rewritable nonvolatile memory 65, there are disposed **electronic wallet** area 708, winning ticket table 709, winning ticket storage area 710, issued lots/betting tickets...

...collected coupon ticket storage area 714, and issued coupon ticket storage area 715.

In the **electronic wallet** area 708, the same types of data as **electronic wallet** area of the customer IC card 2 are stored.

The winning ticket table 709 stores...the POS terminal 1. The POS terminal 1 encrypts this random number using a certain **encryption key** and transmits back to the store IC card 3. The random number transmitted back is...

...is then transmitted to the IC card 3 together with the generated random number. An **encryption** processing **program** in OS area 41 of the IC card 3 encrypts the received random number using an **encryption key** 48 provided in the IC card 3, and the encrypted number is transmitted to the ...

...be transmitted from the POS terminal 1 through the store IC card reader/writer 21.

(**Electronic wallet** transaction processing)

Transaction processing of **electronic wallet** in the store IC card 3 is performed in steps S804 to S809 shown in FIG. 9, while transaction processing of **electronic wallet** in the customer IC card 2 is performed in steps S1204 to S1209 shown in...

...step S208 performed in the POS shown in FIG. 3, when a transaction processing of **electronic wallet** is commissioned from the POS terminal 1 to the store IC card 3, first the...

...memory 35 of the customer IC card 2 and determines whether an access to the **electronic wallet** area 42 is permitted. When the access is permitted, the customer IC card 2 read out the data in the **electronic wallet** area 42 into the nonvolatile memory 34.

Steps S806, S1206:

The customer IC card 2...

...card 2 then subtracts the transaction amount of interest from the balance recorded in the **electronic wallet** area 42 (S1208). The transaction amount is transferred to the store IC card 3 together 3 updates the own **electronic wallet** area 708. Thereafter an exchange completion notification is transmitted to the customer IC card 2...

...the store IC card 3 to the customer IC card 2, the transfer amount is **encrypted** using the **encryption key** and the **encryption program** having been used when performing the previous mutual authentication. In the customer IC card 2, this **encrypted** amount **information** is decrypted to obtain the transaction amount information. Similarly, when the customer IC card 2...

...not only for transferring transaction amount, as described below. As an example, a portion of **data** for communication is **encrypted** first. The entire **information** including the **encrypted data** on the portion concerned is transmitted to the opposite party. On the opposite party side...

...the customer IC card 2 stores the transaction record into the history area in the **electronic wallet** area 42 of the memory 35, and then the **electronic wallet** transaction is completed. The customer IC card 2 is shifted to the command waiting state...

...As for the electronic signature, it is possible to use a signature obtained from the **encrypted data** of coupon ticket **information** , commodity code, discount rate, date of issue in the management source, company code of the management source, and manufacturer code, using a specified **encryption key** . The transfer **information** between the IC cards is **encrypted** using an **encryption key** applied for the mutual authentication.

Step S852, S1233:

The store IC card 3 decrypts the **information** when having been **encrypted** and collects this in step S851. Thereafter in this step S852, the store IC card...electronic signatures respectively attached to the lot and the ticket are also transmitted. As for **information** for transmission, enhanced **security** is considered against wiretapping or forgery. For example, as mentioned earlier, entire **information** or a portion of **information** is **encrypted** using an **encryption key** , or otherwise the entire **information** or a portion of **information** is **encrypted** using an **encryption key** to be added to the entire **information** for transmission. When such **secured** communication is made, procedure necessary for decrypting is inserted in each side of transmission and...step for verifying the access right for the opposite party. Similar to the step described **before** , it is **verified** in this step whether reading, writing and deleting are possible to the coupon information area...

...the encryption logic having been mutually authenticated with the customer IC card 2. For this **encryption** , **encryption key** 706 shown in FIG. 8 is used. Thereafter, in step S815, the store ...2 encrypts the lot number and the electronic signature therefor being extracted from the received **information** , using the **encryption** logic mutually authenticated and the **encryption key** owned in the customer IC card 2. The customer IC card 2 then checks whether or not this **encrypted information** coincides with the electronic signature added by the store IC card 3. If the electronic...

...necessary to apply encrypting by means of encryption logic for use in mutual authentication or **encryption key** for the store IC card 3. It may be possible to use a simple and...stays in the lock condition, it is not possible for the indicator 1500 to access **electronic wallet** data area and lot/betting information area unless PIN identification is not completed. This access...

...lock condition, for example, "LOCK".
Step S1251:
When the IC card 1518 is in the **lock** condition, the customer operates the **key** 1510 of the indicator 1500 to input the personal identification number (PIN). For example, when...

...processing step S1253, first, the IC card 1518 reads out a balance stored in the **electronic wallet** area 42 shown in FIG. 5, and supplies to the indicator 1500 shown in FIG...

...out the first transaction record in the area having the transaction record information of the **electronic wallet** area 42 shown in FIG. 5. This transaction record is supplied to the indicator 1500...the indicator 1500. Here, in a similar manner to the case of reading out the **electronic wallet** area and the lot/betting ticket information area, the electronic signature is not read out...

...If being not in the lock condition, the process returns to the readout step of **electronic wallet** area in step S1253. If, on the other hand, being in the lock condition, the...

...If the personal identification number matches, the process returns to step S1253 in which the **electronic wallet** area is read out. If the personal identification number does not match, the process is...

...processing shown in FIG. 13 is started in each IC card. More specifically, as mentioned **earlier** , it is **verified** whether the equipment being connected is **authorized** equipment in step S1201. Next, in step S1202, it is checked what is equipment being...confirms the additional storing operation into the memory is permitted. Next, in step S1114, by **encrypting** the **information** related to the received lot, the **encryption data** is obtained. The store IC card 3 then compares the **encrypted data** with the electronic signature having been generated by the totaling equipment and transmitted attached at...writer 2109. The IC card 3 receives this information in steps S1113 to S1116 mentioned **earlier** in FIG. 12, and **verifies** and stores into the corresponding area in the memory owned by itself. Thus the transfer...ticket. This procedure is similar to the procedure of electronic signature generation having been explained **earlier** . For the **verification** , the electronic signature generated above is compared with the electronic signature attached to each coupon...

...is verified by checking whether the ticket corresponds to the coupon ticket having been set **before** in the external storage 2105. When the **verification** for the entire coupon tickets is completed, the process proceeds to step S1812 shown in...is obtainable. Therefore, it is possible to perform automatic settlement without implementing a large-scaled **online network** . This will be particularly ...any other service tickets for providing various types of services are applicable.
(3) As for **electronic wallet** transaction equipment, a POS terminal

has been taken as an example of the embodiment. Any other equipment which can handle **electronic wallet** transaction is also applicable.

(4) As for types of services in **electronic wallet** transactions, a discount service has been explained in the above embodiment. However any other services...

...processing transaction data, in particular a backend system for customer service to be accompanied to **electronic wallet** transaction system.

Particularly, transaction data are collected into an IC card and are processed automatic...

...by management equipment. This enables to automate collection and settlement processing without implementing a particular **online network** .

Further, automatic collection and settlement enable to prevent an illegality possibly conducted by either a...

...CLAIMS a card reader/writer (20a) for exchanging information with a customer IC card (2) having **electronic wallet** transaction function;

a card reader/writer (21) for exchanging information with said IC card (3); and

a processing means (17) for performing an **electronic wallet** transaction by transferring **electronic** value in said customer IC card (2) to said IC card (3).

6. The transaction...

...to claim 5 wherein said transaction equipment (1) issues said service information based on said **electronic wallet** transaction.

8. The transaction system according to claim 5 wherein said transaction equipment (1) reflects a service being performed according to said extracted service information to said **electronic wallet** transaction.

9. The transaction system according to claim 6 wherein said management equipment (9) generates...

...3) storing transaction data in a transaction equipment (1) having a memory (65) comprising:

an **electronic wallet** area (708); and

a service information storage area (709) for storing service information provided a...

```
 51/3,K/33     (Item 33 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
```

```
01150452
An  internet  payment and loading system using a smart card
 Internetsystem  zum Zahlen und Laden mit einer Chipkarte
Systeme  de paiement et de rechargement par  Internet , utilisant une carte
    a puce
PATENT ASSIGNEE:
  VISA INTERNATIONAL SERVICE ASSOCIATION, (560813), 900 Metro Center
    Boulevard, Foster City, CA 94404, (US), (Applicant designated States:
    all)
INVENTOR:
  Davis, Virgil M., 1121 Runnymead Drive, Los Altos, CA 94024, (US)
  Cutino, Suzanne C., 431 Arkansas Street, San Francisco, CA 94107, (US)
  Berg, Michael J., 2644 Belmont Canyon Rd, Belmont, CA 94002, (US)
  Conklin, Fredrick Sidney, 26 Alida Court, Oakland, CA 94602, (US)
  Pringle, Steven John, 5174 Miles Avenue, Oakland, CA 94618, (US)
LEGAL REPRESENTATIVE:
  Finnie, Peter John et al (79521), Gill Jennings & Every, Broadgate House,
    7 Eldon Street, London EC2M 7LH, (GB)
PATENT (CC, No, Kind, Date):  EP 1003139  A2  000524 (Basic)
                              EP 1003139  A3  011017
APPLICATION (CC, No, Date):   EP 2000200558 980430;
PRIORITY (CC, No, Date): US 45883 P 970430; US 951614 971016
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI;
  LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
RELATED PARENT NUMBER(S) - PN (AN):
  EP 1023705   (EP 98920079)
INTERNATIONAL PATENT CLASS (V7): G07F-019/00; G07F-007/08;  G06F-017/60
ABSTRACT WORD COUNT: 301
NOTE:
  Figure number on first page: 17

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text  Language    Update    Word Count
      CLAIMS A  (English)  200021      1549
      SPEC A    (English)  200021     19201
Total word count - document A         20750
Total word count - document B             0
Total word count - documents A + B   20750

An  internet  payment and loading system using a smart card
 Internetsystem  zum Zahlen und Laden mit einer Chipkarte
Systeme  de paiement et de rechargement par  Internet , utilisant une carte
    a puce
...INTERNATIONAL PATENT CLASS (V7):  G06F-017/60

...ABSTRACT smart card (5) for payment of goods and/or services purchased
  on-line over the  Internet  (202). A client module on a client terminal
  (204) controls the interaction with a consumer...

...payment server (206). Loading works in conjunction with a bank server
  (860) and a load  server  (862). The  Internet  provides the routing
```

functionality between the client terminal and the various servers. A payment **server** (206) on the **Internet** includes a computer and a security module (or a security card (218) in a terminal...

...an acquirer to accept smart card payments for goods and/or services purchased over the **Internet** . A consumer uses his smart card (5) at the client terminal (204) in order to...

...SPECIFICATION invention relates generally to a payment system and a value loading system using a computer **network** . More specifically, the present invention relates to a payment system and a value loading system for a smart card using an open **network** such as the **Internet** .

Background to the Invention

With the explosive growth in open **networks** (such as the **Internet**) over the past several years and the rapid increase in the number of consumers with access to the **World Wide Web** , there has been a great deal of interest in the development of electronic commerce on the **Internet** . Traditional financial transactions are being transformed.

A variety of service providers have introduced payment schemes...

CLAIMS 1. A loading system for loading value over a **network** onto a stored-value card, said loading system comprising:

a router for routing communication between entities attached to said **network** ;

a bank **server** in communication with said **network** , said bank **server** arranged to debit a user account by an indicated value;

a client terminal in communication with said **network** , said client terminal including a card reader for communicating with a stored-value card and...

...value to debited from said user account; and

a load server in communication with said **network** , said load **server** including an interface for communicating with a security module and being arranged to receive a...

...value card signature and being further arranged to transmit a confirmation message to said bank **server** over said **network** , thereby assuring that said stored-value card has been loaded by said indicated value.

2. A loading system according to claim 1, wherein said **network** is an **internet** and said bank **server** includes a bank **web** site for accepting a load request.

3. A loading system according to claim 1 or...

...said client terminal and said bank server are at separate locations and communicate over said **internet** .

4. A loading system according to any preceding claim, further comprising: a clearing and administration...

...a transaction.

7. A computer-implemented method of loading a stored-value card over a **network** comprising the steps of:

establishing communication between a bank server and a client over a **network** ;

receiving a request from said client to load value onto a stored-value card;

transmitting...

...that the loading is a success.

8. A method according to claim 7, wherein said **network** is an **internet** over which said recited steps of said method occur, wherein said bank **server** includes a bank **web** site for accepting a load request, and wherein said client and said bank server are...

...said confirmation step includes receiving a confirmation message that originates from one of said load **server** and a **security** module associated with said load server.

10. A method according to any of claims 7 to 9, further comprising the steps of:

transmitting a first **key** to said client for **encrypting** a load request to be sent to said load server;

providing said first **key** to decrypt said **encrypted** load request to said load server without sending said first key in the clear to said load server; and

receiving an encrypted confirmation message from said load server that is **encrypted** by a second **key** shared between said bank server and said load server.

11. A method according to any...

...later settlement.

12. A computer-implemented method of loading a stored-value card over a **network** comprising the steps of:

transmitting over a **network** from a client terminal to a bank server a request to load a stored-value...

...from said bank server a verified load value;

sending a load request to a load **server** connected to said **network** ;

receiving a load command from said load server;

loading said stored-value card by said...

...that said loading is a success.

13. A method according to claim 12, wherein said **network** is an **internet** over which said recited steps of said method occur, wherein said bank **server** includes a bank **web** site for accepting a load request, and wherein said client terminal and said bank server...

...load request so that said responses may be sent as a group to said load **server** to reduce **network** traffic between said load server and said client terminal.

15. A method according to any of claims 12 to 14, wherein said confirmation **information** includes an **encrypted** confirmation message unreadable by said client terminal, said method further comprising:

receiving said encrypted confirmation...

...of managing a stored-value card load transaction between a client terminal and a bank **server** connected over a **network** , said method comprising the steps of:

receiving by a load **server** over said **network** a load request, said load request including a stored-value card signature;

sending said stored...that the loading is a success.

17. A method according to claim 16, wherein said **network** is an **internet** over which said recited steps of said method occur, wherein said bank **server** includes a bank **web** site for accepting a load request, and wherein said client terminal and said bank server...

...in an interaction with said security module to receive responses from said security module, whereby **network** traffic between said load server and said client terminal is reduced.

19. A method according...

...by a client terminal to facilitate the loading of said stored-value card over a **network** , said method comprising the steps of:

receiving a load value from a bank **server** connected to said **network** ;

emulating a plurality of security module commands that are sent to said stored-value card...

...value card to form a load request; and

sending said load request to a load **server** over said **network** so that said load request may be processed by a security module associated with said load server to facilitate the loading of said stored-value card over said **network** , whereby **network** traffic between said load server and said client terminal is reduced.

21. A method according to claim 20, wherein said **network** is an

internet over which said recited steps of said methodoccur, wherein said bank **server** includes a bank **web** site for accepting a load request, and wherein said client terminal and said bank server...

...by a load server to facilitate the loading of a stored-value card over a **network** , said method comprising the steps of:
receiving a load request from a client terminal over a **network** , said load request including a plurality of responses from a stored-value card generated in response to emulation of security module commands, whereby **network** traffic between said load server and said client terminal is reduced;
emulating said stored-value...

...to said emulation; and
sending a load command destined to said client terminal over said **network** to facilitate loading of said stored-value card.
24. A method according to claim 23, wherein said **network** is an **internet** over which said recited steps of said method occur, and wherein said client terminal and...

51/3,K/38 (Item 38 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00557647 **Image available**
CARD FOR INTERACTION WITH A COMPUTER
CARTE PERMETTANT D'INTERAGIR AVEC UN ORDINATEUR
Patent Applicant/Assignee:
COMSENSE TECHNOLOGIES LTD,
ANTEBI Amit,
ATSMON Alon,
LEV Zvi,
COHEN Moshe,
Inventor(s):
ANTEBI Amit,
ATSMON Alon,
LEV Zvi,
COHEN Moshe,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200021020 A2 20000413 (WO 0021020)
Application: WO 99IL525 19991004 (PCT/WO IL9900525)
Priority Application: IL 126444 19981002; IL 127072 19981116; IL 127569 19981214; US 99115231 19990108; US 99122687 19990303; US 99143220 19990709; US 99145342 19990723; WO 99IL470 19990827; US 99153858 19990914; WO 99IL506 19990916; WO 99IL521 19991001
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB
GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD
MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG
US US US US US US US US UZ VN YU ZA ZW GH GM KE LS MW SD SL SZ TZ UG ZW
AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC
NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 22786

Main International Patent Class (v7): **H04L-009/00**
Fulltext Availability:
Detailed Description
Claims

Detailed Description
... especially to cards that use acoustic signals for such communications.

BACKGROUND OF THE INVENTION
Computer **network** components that communicate using RF radiation, wires or IR radiation are well known. Dedicated ultrasonic...

...to increase bandwidth and reduce noise.

However, such dedicated communication mechanisms require that the computer **network** components have installed thereon specialized communication hardware. Installing such hardware on an existing computer may...

...microphone of a telephone using a DTMF-like encoding scheme. A VAVW page addressed "http:// **www** .encotone.com/html/tech - deflitnil", available February 1, 1999, but possibly published prior to that...

...may interpret signals from a smart-card, rather than transmitting them on through the telephone **network** , as in the prior art.

However, in other embodiments the sound communication is alternatively or ...card and an electronic device, comprising.

providing a smart card;
7
interaction software from said **Internet** .
In a preferred embodiment of the invention, said interaction software retrieves information from said smart card and inserts said information in at least one field of a **WWW** form displayed on said computer. Alternatively or additionally, said interaction software retrieves information form said...display that displays pertinent information regarding the transaction, retrieved via said link from said computer, **prior** to **authentication** of said transaction by the smart card.

Preferably, said display comprises a visual display. Alternatively...

...with a preferred
embodiment of the invention;
Fig. 4A is a schematic illustration of an **Internet** transmission pathway for sounds, in
accordance with a preferred embodiment of the invention;
Fig. 4B...by the card causing a browser executing on an associated computer to present a particular **WWW** page to the user, based on the required help. The help may be context-sensitive...

...of a device component, for example using a bar code.

26
USE OF CARD FOR **ELECTRONIC WALLET**
It should be noted that such an acoustic smart-card may also be used as a customer card, as well as for an " **electronic wallet** ", since information about the card holder can easily be retrieved from the card. Also, it...the response of the card to a more remote object, for io example over an **Internet** . For identification purposes, the card may send an ID code even without prompting from the...

...be used to give privileges to a card's owner in the form of better **Internet** service (speed of connection, limits). For example, a manager can come to his employee desk, wave his card and the **Internet** connection will be better. Alternatively,
29
various security restrictions may be alleviated, using the manager...

...a computer. The card transmits authentication information (for example a one-time code) to an **Internet server** and that **server** signs on the transaction.

Alternatively or additionally, a "bionietrics authority" is provided, which authority knows...
...The information sent to the authority can be asymmetrically encrypted.

SMART-CARD TRANSMISSION OVER A **NETWORK**
Fig. 4A is a schematic illustration of an **Internet** transmission pathway for sounds, in accordance with a preferred embodiment of the invention. When a...

...of the invention, a local client computer 62 receives sounds and transmits them over an **Internet** 60 to a **server** computer 50. Alternatively to using an **Internet** , an Intranet, a LAN, a **WAN** or another type of computer data **network** is used. Alternatively or additionally, at least part of the transmission path may comprise telephone...

...from the card. It is noted that there exist standard protocols for transmitting sounds over **networks** . Thus, there is little or no need for changes in the hardware and/or software...

...the smart-card. It is noted that playing of sound is also supported by standard **Internet** protocols.

Alternatively or additionally, a smart-card may serve as an interrogated ID card that is used to control access to and/or billing of usage of an **Internet** site. In one example, whenever a user requests a service from the **Internet** , the existence of a local smart-card is ascertained.

Billincr information is preferably transmitted to...

...card. Preferably, the card is interrogated periodically (possibly by a third party), preferably over the **Internet** or a telephone connection, for the existence of charges. Alternatively, a debit card may be...

...interrogation is necessarily required.

In an example of a financial or business interaction over an **Internet** , one or more of the following three levels of security may be achieved. First, the...

...electronic device) may include encrypted communications, for example using RSA, DES, triple DES or TEF **encoding** or other public- **key** algorithms. Alternatively or additionally, the communication may use DTMF or DTMF-like tones. Alternatively or paper slip to be signed. However, a digital-type signature is preferred. In an **electronic** **wallet** situation, no credit card company is used. Instead "cash" is withdrawn from the smart-card...

...embodiment of the invention, the tap is placed on a cable to a printer, a **network** cable, a camera cable and/or a SCSI connection. Additionally or alternatively, the tap is...

...output signals on an input line, such as a mouse). Additionally or alternatively, the signals **encode** **information** which **information** is detected and removed from the data stream in the computer. Additionally or alternatively, the...Preferably, the software is self installing, for example from a zipped file or from the **Internet** as a downloaded software component. Preferably, the computer is not used for any other use...

...user 146 wishes to interrogate computer 140, for example to determine the presence of a **networking** problem. In a preferred embodiment of the invention, a smart-card 144 (or other electronic performed. The received information may be decrypted (if necessary). Alternatively or additionally, the received **information** may be **encrypted** , verified and/or signed, in order to be stored in local memory. The local memory...

...37
RAM, EPROM, EPROM and/or other types of memory as known in the art. **Information** to be transmitted may be **encrypted** before transmission.

An exemplary **software** for the PC receives a detected signal, filters it, and opens the protocol. Preferably, the...

Claim
... is two-way.

41 A system according to claim 38, comprising a connection to the **Internet** .

42 A system according to claim 41, wherein said computer comprises a **network** software for downloading said interaction software from said **Internet** .

43 A system according to any of claims 38-42, wherein said interaction software retrieves...

...from said smart card and inserts said information in at least one field of a **WWW**
57
. A system according to any of claims 38-42, wherein said interaction software retrieves...

...from said smart card and controls a browser on said computer to show a particular **WWW** page responsive to said information.
45 A smart card comprising:
a memory;
a text-to...for powering processing of data.

69 A method acquiring to claim 68, wherein said waves **encode** said **data** .
60
. A method according to claim 68 or claim 69, wherein transmitting compnses transmitting from...

...into energy; and
utilizing said energy by said smart card, for powering the processing of **data** , wherein said waves **encode** said **data** .

72 A method according to claim 71, comprising transmitting a result of said processing from...display that displays pertinent information regarding the transaction, retrieved via said link from said computer, **prior** to **authentication** of said transaction by the smart card. 125. A smart card according to claim 124...

51/3,K/43   (Item 43 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00493543   **Image available**
TAMPER RESISTANT METHOD AND APPARATUS
APPAREIL ET PROCEDE ANTI-EFFRACTION

Patent Applicant/Assignee:
  CYBERCASH INC,
Inventor(s):
  ELLISON Carl,
Patent and Priority Information (Country, Number, Date):
  Patent: WO 9924895 A1 19990520
  Application: WO 98US23437 19981103 (PCT/WO US9823437)
  Priority Application: US 97965595 19971106
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
  AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH
  GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW
  MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW GH
  GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES
  FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN
  TD TG
Publication Language: English
Fulltext Word Count: 4852

Main International Patent Class (v7): **G06F-001/00**
Fulltext Availability:
  Detailed Description
  Claims

English Abstract

A method for **securing** **data** in a tamper resistant fashion on a computer connected to a **network** . The presence of a user on a **network** is established using one protocol with routine operations conducted by the user on the **network** using a second protocol. Public and private **key** **encryption** is used to establish the validity of both the user and the **server** on the **network** user on the **network** . Keys are passed only after verification of the authenticity of the user on the **network** .

Detailed Description
... of the Invention
This invention relates generally to methods of secure electronic commerce over a **network** . More specifically the invention relates to a method and apparatus for achieving tamper resistant status for commercial transactions over a **network** .

Background

Commerce has become increasingly electronic in nature with wire transfer of funds a common occurrence. Further the use of open **networks** , such as the **Internet** , has become a primary vehicle by which electronic commerce takes place. With the increase in...tampered with, falsified and fraudulently conducted

In response to the potential for fraud on the **Internet** various inventions have been generated to secure the transactions of users. For example, the concept of a " **wallet** " which i an **electronic** version of money held by a user is protected in part by a private key...

...the user. The private key is kept secret since the key is part of wallet **data** which is **encrypted** and stored in a computer. In normal implementations, the **encryption key** that protects the wallet **data** is generated by a cryptographic hash ...the event that the passphraseis discovered

Security can be improved by storing the especially private **data** (such as private **encryption keys**) in a hardware **token** . Such hardware tokens as smartcards, or PCMCIA cards are ...is validated to perform the desired interaction. This validation includes establishing a one time session **key** used to **encrypt** certain **information** passed between the stored value card and the terminal. In addition a range of **encryption** techniques using **data encryption** standard **keys** are incorporated. Though
2
the dual challenge procedure of '642 is somewhat similar to the challenge process of the present invention, the integration of the challenge process and signature **keys** with symmetric **key encryption** of the present invention is not disclosed

United States Patent No. 5,568,552, issued...

...devices to accomplish the objectives. The '552 invention distributes the key material through-out the **network** and does not disclose a method whereby the key **information** is held in a more **secure** in at a single location

United States Patent No. 5,557,678 issued to Ganesan challenge process and signature **keys** with symmetric **key encryption** of the present Invention is not disclosed

United States Patent No. 5,483,596 issued...by the devices to establish a communications link. Integration of the challenge process and signature **keys** with
symmetric **key encryption** of the present invention is not disclosed

United States Patent No. 5,469,507 issued the presence of multiple processors in a **network** system, with a form of voting or corroboration from and between each of the processors...to Diffie, et al. discloses a method for authentication between two users on a wireless **network** . The '794 invention discloses a series of authentication steps coupled with random ...authentication and security between two users. The '840 invention does not require storage of a **cypher key** at the remote computer and the remote user code or PIN is not transferred between...

...that established the authentication as the session key. Integration of the challenge Process and signature **keys** with symmetric **key encryption** of the present invention is not disclosed

It is therefore an object of the present on a Personal Computer, provided only that it is connected to a **network**

It is a further object of the present invention to provide enhanced security and tamper resistance to **networks** using public and private **key encryption** of transactions

It is a further object of the present invention to limit the ability of an active eavesdroppe .21 to access information from the server on the tamper resistant **network** of the present invention

It is a further object of the present invention to enhance the security associated with the .use of public and private **key** **encryption** of transactions

It is a further object of the present invention to employ the **networked** tamper resistance server in a challenge response mode thereby authenticating the validity of users on the **network**

It is a further object of the present invention to pass symmetric **keys** in. **encrypted** form t users only after verification of the authenticity of the user on a **network**

It is a further object of the present invention to increase exponentially the time between unsuccessful attempts by a party to access the **network**

Claim
What is claimed is:

1. A tamper resistant method for **securing** a user's **data** comprising:
Initializing the presence of at least one user on a tamper resistant **networked** device using
a first protocol; and
Establishing routine operations by the user on the **network** using a second protocol. .

2. The tamper resistant method for securing **networks** of claim 1 wherein the first protocol
comprises:
the user sending a message to a **network** **server** ;
the **server** verifying the presence of a user record;
the server creating a new record if an...and sending the encrypted passphrase back to the server; and
the server generating a symmetric **key** , the symmetric **key** **encrypted** by the server and sent to the user.

3. The tamper resistant method for **securing** a user's **data** of claim 1 ...sending a first message to the server identifying the presence of the user on the
network ;
the **server** looking up the record of the user to verify the user is permitted access;
the...

...to the server;
the server checking the signed challenge;
the server generating a temporary symmetric **key** and sending the temporary symmetric **key** back to the user, **enciphered** in a confidentiality **key** of the user's known to the server;
the user receiving the temporary symmetric key...

...the challenge from the server;
the user encrypting the users passphrase using the temporary symmetric **key** and sending
the **encrypted** passphrase to the server;
the server decrypting the encrypted passphrase and checking the passphrase against...a symmetric key to the user for subsequent use.

4. The tamper resistant method for **securing** a user's **data** of claim 3 wherein the first user message comprises the user's public key, and a transaction identifier.

5. The tamper resistant method for **securing** a user's **data** of claim 3 wherein the server looking up the record of the user further comprises tamper resistant method for **securing** a user's **data** of claim 5 wherein further comprising the server ignoring the message if no record of the user exists.

7. The tamper resistant method for **securing** a user's **data** of claim 5 further comprising ignoring the message if the next permitted interaction time associated...
...the user is greater than the present server time.

8. The tamper resistant method for **securing** a user's **data** of claim 3 further comprising the server sending a random challenge to the user only time associated with the user.

9. The tamper resistant method for **securing** a user's **data** of claim 3 wherein the random challenge generated by the serve sent to the user further comprises the transaction ID.

10. The tamper resistant method for **securing** a user's **data** of claim 3 wherein the user signing the challenge message further comprises the user signing the message with the user's private key.

11. The tamper resistant method for **securing** a user's **data** of claim 3 wherein the checking of the signed challenge further comprises ignoring the user message if the signed challenge response is incorrect.

12. The tamper resistant method for **securing** a user's **data** of claim 3 wherein the server generating a temporary symmetric **key** further comprises **encrypting** the temporary symmetric **key** using the public key of the user.

13. The tamper resistant method for **securing** a user's **data** of claim 12 wherein the user receiving the temporary symmetric key further comprises the user decrypting the **encrypted** temporary symmetric **key** using the user's private key.

14. The tamper resistant method for **securing** a user's **data** of claim 2 wherein the user message further comprises the ...transaction identifier, and a request for a new record.

15. The tamper resistant method for **securing** a user's **data** of claim 2 wherein verifying the
presence of a record by the server comprises using...

...s
public key to determine if a
record exists.

16. The tamper resistant method for **securing** a-user's **data** of claim 15 wherein verifying the presence of a record further comprises ignoring the user message if a record exists.

17. The tamper resistant method for **securing** a user's **data** of claim 2 wherein the server sending the session key back to the user further comprises **encrypting** the session **key** with the public key if the user.

18. The tamper resistant method for **securing** a user's **data** of claim 2 wherein the user encrypting the passphrase further comprises **encrypting**

the passphrase with the session **key** .

19. The tamper resistant method for **securing** a user's **data** of claim 2 wherein the sending of the symmetric **key** to the user further comprises **encrypting** the symmetric **key** using the session key.

```
Set     Items   Description
S1    3245208   (STORAG? OR WEB OR CACHE?? OR CACHING OR SECUR? OR NETWORK
             OR INTERNET?)(3N)SERVER OR WEBSITE OR WEBPAGE OR ETHERNET? OR
             EXTRANET? OR WWW OR WORLD()WIDE()WEB OR WORLDWIDEWEB OR SUBNE-
             T? OR WAN? ? OR ONLINE OR INTERNET? OR NETWORK?
S2     199595   (SECUR? OR ENCOD? OR ENCRYPT? OR CIPHER? OR CYPHER? OR ENC-
             IPHER? OR ENCYPHER? OR LOCK???)(5N)(ELECTRONIC()WALLET? OR KE-
             Y??? OR CONTAIN??? OR DIGITAL()OBJECT? OR TOKEN? OR DATA OR D-
             ATA()FILE? ? OR INFORMATION?? OR SOFTWARE? OR PROGRAM? OR VPN-
             ??) OR PERSONA
S3       1573   (REQUEST? OR INQUIR? OR QUERY? OR QUERIES OR ASK??? OR REQ-
             UIS? OR DEMAND??? OR SEEK???)(5N)S2
S4      89100   (DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR T-
             RANSFER? OR TRANSMIT? OR BEAM??? OR PROVID?)(5N)(IDENTIF? OR -
             IDENTIT?)
S5      16926   (DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR T-
             RANSFER? OR TRANSMIT? OR BEAM??? OR PROVID?)(5N)S2
S6       5575   (RECEIV? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR DOWNLOAD? OR -
             PULL???()DOWN?? OR PROCUR??? OR GET? ? OR FETCH??? OR RETRIEV-
             ?)(5N)S2
S7     187334   (CERTIFICAT? OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUT-
             HORIZ? OR AUTHORIS? OR APPROV? OR VERIF? OR KEY??? OR PASSWOR-
             D??)(5N)SERVER?? OR SERVER?
S8      64090   (DECRYPT? OR DECIPHER? OR DECOD? OR UNLOCK? OR CERTIFICAT?
             OR AUTHENTICAT? OR VERIF?)(3N)(KEY??? OR DEVICE OR MECHANISM??
              OR PASSWORD?? OR CODE? ? OR CODING OR ACCESS?)
S9        431   (REQUEST? OR INQUIR? OR QUERY? OR QUERIES OR ASK??? OR REQ-
             UIS? OR CHALLENG??? OR DEMAND??? OR SEEK???)(5N)S8
S10       428   ((DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR -
             TRANSFER? OR TRANSMIT? OR BEAM??? OR PROVID?)(5N)(CERTIFICAT?
             OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUTHORIZ? OR AUTHOR-
             IS? OR VERIF?))(5N)S7
S11      3805   (DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR T-
             RANSFER? OR TRANSMIT? OR BEAM??? OR PROVID?)(5N)S8
S12      1951   (RECEIV? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR DOWNLOAD? OR -
             PULL???()DOWN?? OR PROCUR??? OR GET? ? OR FETCH??? OR RETRIEV-
             ?)(5N)S8
S13   1682766   CERTIFICAT? OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUTH-
             ORIZ? OR AUTHORIS? OR APPROV? OR VERIF?
S14       416   ((BEFORE? OR PRIOR? OR EARLIER? OR ADVANCE? OR IN()ADVANCE
             OR AHEAD? OR SUBSEQUEN? OR ALREADY?)(5W)(RECEIV? OR ACCEPT? OR
              ACQUIR? OR OBTAIN? OR DOWNLOAD? OR PULL???()DOWN?? OR PROCUR-
             ??? OR GET? ? OR FETCH??? OR RETRIEV?))(10W)S13
S15         2   S5 AND S14
S16         0   S12 AND S14
S17     30814   S1(10N)S2
S18       163   S17 AND S7(10N)S8
S19         0   S18 AND S14
S20         0   S6 AND S14
S21         3   S2 AND S14
S22        21   S18 AND S2/TI
S23        19   RD  (unique items)
S24        19   S17 AND S6 AND S12
S25        24   S21:S23
S26        19   S24 NOT S25
S27        15   RD  (unique items)
S28         6   S27 NOT PY>1999
S29       215   S14 NOT PY>1999
S30       187   RD  (unique items)
S31         0   S30 AND S4
S32         0   S30 AND S7
```

```
S33          2   S30 AND S8
S34        163   S1(10N)S2 AND S7(10N)S8
S35         24   S34 AND S3:S6 AND S9:S12
S36         12   S35 NOT PY>1999
S37         11   RD  (unique items)
S38         45   S15 OR S21:S28 OR S33
S39         10   S37 NOT S38
S40      26538   ((SECUR? OR ENCOD? OR ENCRYPT? OR CIPHER? OR CYPHER? OR EN-
             CIPHER? OR ENCYPHER? OR LOCK???)(5N)(EMAIL? OR E()MAIL? OR EL-
             ECTRONIC()WALLET? OR KEY??? OR CONTAIN??? OR DIGITAL()OBJECT?
             OR TOKEN? OR DATA OR DATA()FILE? ? OR INFORMATION?? OR SOFTWA-
             RE? OR PROGRA
S41      26538   S1(5N)S40
S42         18   S41 AND S6 AND S12
S43         64   S35:S39
S44          2   S42 NOT S43
File   2:INSPEC 1898-2006/Mar W2
         (c) 2006 Institution of Electrical Engineers
File   6:NTIS 1964-2006/Mar W2
         (c) 2006 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2006/Mar W2
         (c) 2006 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2006/Mar W2
         (c) 2006 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2006/Feb
         (c) 2006 ProQuest Info&Learning
File  62:SPIN(R) 1975-2006/Mar W1
         (c) 2006 American Institute of Physics
File  65:Inside Conferences 1993-2006/Mar 21
         (c) 2006 BLDSC all rts. reserv.
File  94:JICST-EPlus 1985-2006/Dec W4
         (c)2006 Japan Science and Tech Corp(JST)
File  95:TEME-Technology & Management 1989-2006/Mar W3
         (c) 2006 FIZ TECHNIK
File  99:Wilson Appl. Sci & Tech Abs 1983-2006/Feb
         (c) 2006 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2006/Mar 13
         (c) 2006 The Gale Group
File 144:Pascal 1973-2006/Feb W4
         (c) 2006 INIST/CNRS
File 239:Mathsci 1940-2006/Apr
         (c) 2006 American Mathematical Society
File 256:TecInfoSource 82-2006/Feb
         (c) 2006 Info.Sources Inc
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
```

```
Set      Items   Description
S1     3240906   WEBSITE OR WEBPAGE OR ETHERNET? OR EXTRANET? OR WWW OR WOR-
              LD()WIDE()WEB OR WORLDWIDEWEB OR SUBNET? OR WAN? ? OR ONLINE -
              OR INTERNET? OR NETWORK?
S2       28816   (STORAG? OR WEB OR CACHE?? OR CACHING OR SECUR? OR NETWORK
              OR INTERNET?)(3N)SERVER
S3       39903   (SECUR? OR ENCOD? OR ENCRYPT? OR CIPHER? OR CYPHER? OR ENC-
              IPHER? OR ENCYPHER? OR LOCK???)(5N)(EMAIL? OR E()MAIL? OR ELE-
              CTRONIC()WALLET? OR KEY??? OR CONTAIN??? OR DIGITAL()OBJECT? -
              OR TOKEN?)
S4      171410   (SECUR? OR ENCOD? OR ENCRYPT? OR CIPHER? OR CYPHER? OR ENC-
              IPHER? OR ENCYPHER? OR LOCK???)(5N)(DATA OR DATA()FILE? ? OR -
              INFORMATION?? OR SOFTWARE? OR PROGRAM? OR VPN??) OR PERSONAL(-
              )SECUR?()DEVICE
S5     1521035   REQUEST? OR INQUIR? OR QUERY? OR QUERIES OR ASK??? OR REQU-
              IS? OR DEMAND??? OR SEEK???
S6       89100   (DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR T-
              RANSFER? OR TRANSMIT? OR BEAM??? OR PROVID?)(5N)(IDENTIF? OR -
              IDENTIT?)
S7    13665351   DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR TR-
              ANSFER? OR TRANSMIT? OR BEAM??? OR PROVID?
S8     8897364   RECEIV? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR DOWNLOAD? OR P-
              ULL???()DOWN?? OR PROCUR??? OR GET? ? OR FETCH??? OR RETRIEV?
S9      187334   (CERTIFICAT? OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUT-
              HORIZ? OR AUTHORIS? OR APPROV? OR VERIF? OR KEY??? OR PASSWOR-
              D??)(5N)SERVER?? OR SERVER?
S10      64090   (DECRYPT? OR DECIPHER? OR DECOD? OR UNLOCK? OR CERTIFICAT?
              OR AUTHENTICAT? OR VERIF?)(3N)(KEY??? OR DEVICE OR MECHANISM??
               OR PASSWORD?? OR CODE? ? OR CODING OR ACCESS?)
S11      63943   (DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR T-
              RANSFER? OR TRANSMIT? OR BEAM??? OR PROVID?)(5N)(CERTIFICAT? -
              OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUTHORIZ? OR AUTHOR-
              IS? OR VERIF?)
S12    1682766   CERTIFICAT? OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUTH-
              ORIZ? OR AUTHORIS? OR APPROV? OR VERIF?
S13    4892171   BEFORE? OR PRIOR? OR EARLIER? OR ADVANCE? OR IN()ADVANCE OR
               AHEAD? OR SUBSEQUEN? OR ALREADY?
S14      31198   S1:S2(10N)S3:S4
S15       5744   S14 AND S5:S7(10N)S3:S4
S16        141   S15 AND S9 AND S10
S17          0   S16 AND S8(10N)S3:S4 AND S8(10N)S12
S18         67   S16 AND S11
S19         11   S18 AND S8 AND S10
S20          6   S19 NOT PY>1999
S21          6   RD  (unique items)
S22      20988   S13 AND S3:S4
S23       2684   S22 AND S7(10N)S3:S4
S24         26   S23 AND S13(10N)S10
S25          9   S24 NOT PY>1999
S26          6   RD  (unique items)
S27        172   S23 AND S7(10N)S3:S4 AND S7(10N)S11
S28        142   S27 AND S7(5N)S3:S4 AND S7(5N)S11
S29         59   S28 AND S13 AND S7 AND S10
S30         25   S29 NOT PY>1999
S31         26   S24:S26
S32         20   S30 NOT S31
S33         17   RD  (unique items)
S34        142   S22 AND S7(5N)S3:S4 AND S7(5N)S11
S35          0   S34 NOT S23
S36          7   S1:S2 AND S7(5N)S3:S4 AND S7(5N)S11 AND S13(10W)S7(10N)S10
S37        259   AU=(DUANE W? OR DUANE, W?)
```

Bib Npl #2

```
S38          0   AU=(ROSTIN P? OR ROSTIN, P?)
S39         22   (WILLIAM OR BILL OR BILLY)(2N)DUANE OR (PETER OR PETE)(2N)-
               ROSTIN
S40        281   S37:S39
S41          0   S37 AND S38
S42          2   S40 AND S1:S2
S43          2   S42 NOT PY>1999
S44          2   S40 AND S1:S4
S45         41   S1 AND S2(10N)S3:S4 AND S9(10N)S10
S46          0   S45 AND S8(10N)S3:S4 AND S13(10N)S10
S47          0   S45 AND S13(10N)S10
S48         13   S45 NOT PY>1999
S49         12   RD  (unique items)
File   2:INSPEC 1898-2006/Mar W2
         (c) 2006 Institution of Electrical Engineers
File   6:NTIS 1964-2006/Mar W2
         (c) 2006 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2006/Mar W2
         (c) 2006 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2006/Mar W2
         (c) 2006 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2006/Feb
         (c) 2006 ProQuest Info&Learning
File  62:SPIN(R) 1975-2006/Mar W1
         (c) 2006 American Institute of Physics
File  65:Inside Conferences 1993-2006/Mar 21
         (c) 2006 BLDSC all rts. reserv.
File  94:JICST-EPlus 1985-2006/Dec W4
         (c)2006 Japan Science and Tech Corp(JST)
File  95:TEME-Technology & Management 1989-2006/Mar W3
         (c) 2006 FIZ TECHNIK
File  99:Wilson Appl. Sci & Tech Abs 1983-2006/Feb
         (c) 2006 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2006/Mar 13
         (c) 2006 The Gale Group
File 144:Pascal 1973-2006/Feb W4
         (c) 2006 INIST/CNRS
File 239:Mathsci 1940-2006/Apr
         (c) 2006 American Mathematical Society
File 256:TecInfoSource 82-2006/Feb
         (c) 2006 Info.Sources Inc
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
```

43/3,K/1   (Item 1 from file: 2)
DIALOG(R)File   2:INSPEC

07025936   INSPEC Abstract Number: C9810-6150N-090
Title: Embed user values in system architecture: the Declaration of System Usability
Author(s): Comstock, E.M.; **Duane, W.M.**
Author Affiliation: Digital Equipment Corp., Littleton, MA, USA
Conference Title: Human Factors in Computing Systems. Common Ground. CHI 96 Conference Proceedings   p.420-7
Editor(s): Tauber, M.J.; Bellotti, V.; Jeffries, R.; Mackinlay, J.D.; Nielsen, J.
Publisher: ACM, New York, NY, USA
Publication Date: 1996 Country of Publication: USA   xii+524 pp.
ISBN: 0 89791 777 4   Material Identity Number: XX96-00860
U.S. Copyright Clearance Center Code: 0 89791 777 4/96/04..$3.50
Conference Title: Proceedings of CHI 96. Human Factors in Computing Systems
Conference Sponsor: ACM
Conference Date: 13-18 April 1996   Conference Location: Vancouver, BC, Canada
Language: English
Subfile: C
Copyright 1998, IEE
Author(s): Comstock, E.M.; **Duane, W.M.**
...Abstract: and usability. This paper shares an effort to embed usability within the architecture of complex **network** products. We began by attempting to build a conceptual model, but we ended by representing...
Descriptors: **network** operating systems...
...Identifiers: complex **network** products...

... **networked** computing

```
Set     Items   Description
S1    24401887   WEBSITE OR WEBPAGE OR ETHERNET? OR EXTRANET? OR WWW OR WOR-
             LD()WIDE()WEB OR WORLDWIDEWEB OR SUBNET? OR WAN? ? OR ONLINE -
             OR INTERNET? OR NETWORK?
S2      518759    (STORAG? OR WEB OR CACHE?? OR CACHING OR SECUR? OR NETWORK
             OR INTERNET?)(3N)SERVER
S3     2318117    (CERTIFICAT? OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUT-
             HORIZ? OR AUTHORIS? OR APPROV? OR VERIF? OR KEY??? OR PASSWOR-
             D??)(5N)SERVER?? OR SERVER?
S4      508620   S1 AND S2 AND S3

S5       32290    (SECUR? OR ENCOD? OR ENCRYPT? OR CIPHER? OR CYPHER? OR ENC-
             IPHER? OR ENCYPHER? OR LOCK???)(5N)(EMAIL? OR E()MAIL? OR ELE-
             CTRONIC()WALLET? OR KEY??? OR CONTAIN??? OR DIGITAL()OBJECT? -
             OR TOKEN?)
S6       98973    (SECUR? OR ENCOD? OR ENCRYPT? OR CIPHER? OR CYPHER? OR ENC-
             IPHER? OR ENCYPHER? OR LOCK???)(5N)(DATA OR DATA()FILE? ? OR -
             INFORMATION?? OR SOFTWARE? OR PROGRAM? OR VPN??) OR PERSONAL(-
             )SECUR?()DEVICE
S7      222580   REQUEST? OR INQUIR? OR QUERY? OR QUERIES OR ASK??? OR REQU-
             IS? OR DEMAND??? OR SEEK???
S8        7984    (DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR T-
             RANSFER? OR TRANSMIT? OR BEAM??? OR PROVID?)(5N)(IDENTIF? OR -
             IDENTIT?)
S9      447884   DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR TR-
             ANSFER? OR TRANSMIT? OR BEAM??? OR PROVID?
S10     297951   RECEIV? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR DOWNLOAD? OR P-
             ULL???()DOWN?? OR PROCUR??? OR GET? ? OR FETCH??? OR RETRIEV?
S11      18483    (DECRYPT? OR DECIPHER? OR DECOD? OR UNLOCK? OR CERTIFICAT?
             OR AUTHENTICAT? OR VERIF?)(3N)(KEY??? OR DEVICE OR MECHANISM??
              OR PASSWORD?? OR CODE? ? OR CODING OR ACCESS?)
S12      30899    (DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR T-
             RANSFER? OR TRANSMIT? OR BEAM??? OR PROVID?)(5N)(CERTIFICAT? -
             OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUTHORIZ? OR AUTHOR-
             IS? OR VERIF?)
S13     141056   CERTIFICAT? OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUTH-
             ORIZ? OR AUTHORIS? OR APPROV? OR VERIF?
S14     276104   BEFORE? OR PRIOR? OR EARLIER? OR ADVANCE? OR IN()ADVANCE OR
              AHEAD? OR SUBSEQUEN? OR ALREADY?
S15      48343   S7:S10(10N)S5:S6
S16        377   S15 AND S7(10N)S11
S17         92   S16 AND S12(10N)S3
S18         33   S17 AND S10(10N)S11
S19         23   S18 NOT PD>1999
S20         18   RD  (unique items)
S21         38   S8(10N)S3:S4 AND S8(10N)S12 AND S13(10N)S8(10N)S10
S22         19   S21 NOT PD>1999
S23         11   RD  (unique items)
S24         10   S23 NOT S20
File   9:Business & Industry(R) Jul/1994-2006/Mar 17
         (c) 2006  The Gale Group
File  13:BAMP 2006/Mar W2
         (c) 2006  The Gale Group
File  15:ABI/Inform(R) 1971-2006/Mar 21
         (c) 2006 ProQuest Info&Learning
File  16:Gale Group PROMT(R) 1990-2006/Mar 21
         (c) 2006 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2006/Mar 20
         (c) 2006 The Gale group
File  75:TGG Management Contents(R) 86-2006/Mar W2
         (c) 2006 The Gale Group
```

```
File  88:Gale Group Business A.R.T.S. 1976-2006/Mar 14
         (c) 2006 The Gale Group
File  98:General Sci Abs 1984-2004/Dec
         (c) 2005 The HW Wilson Co.
File 141:Readers Guide 1983-2004/Dec
         (c) 2005 The HW Wilson Co
File 148:Gale Group Trade & Industry DB 1976-2006/Mar 20
         (c)2006 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 275:Gale Group Computer DB(TM) 1983-2006/Mar 20
         (c) 2006 The Gale Group
File 369:New Scientist 1994-2006/Aug W4
         (c) 2006 Reed Business Information Ltd.
File 370:Science 1996-1999/Jul W3
         (c) 1999 AAAS
File 484:Periodical Abs Plustext 1986-2006/Mar W2
         (c) 2006 ProQuest
File 553:Wilson Bus. Abs. 1982-2006/Mar
         (c) 2006 The HW Wilson Co
File 610:Business Wire 1999-2006/Mar 21
         (c) 2006 Business Wire.
File 613:PR Newswire 1999-2006/Mar 21
         (c) 2006 PR Newswire Association Inc
File 621:Gale Group New Prod.Annou.(R) 1985-2006/Mar 20
         (c) 2006 The Gale Group
File 624:McGraw-Hill Publications 1985-2006/Mar 21
         (c) 2006 McGraw-Hill Co. Inc
File 634:San Jose Mercury  Jun 1985-2006/Mar 20
         (c) 2006 San Jose Mercury News
File 635:Business Dateline(R) 1985-2006/Mar 21
         (c) 2006 ProQuest Info&Learning
File 636:Gale Group Newsletter DB(TM) 1987-2006/Mar 20
         (c) 2006 The Gale Group
File 647:CMP  Computer Fulltext 1988-2006/Apr W2
         (c) 2006 CMP Media, LLC
File 674:Computer News Fulltext 1989-2006/Mar W2
         (c) 2006 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2006/Mar 21
         (c) 2006 Dialog
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
```

20/3,K/4 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

07383765 Supplier Number: 61414708 (USE FORMAT 7 FOR FULLTEXT)
Security Systems.
Bank Systems + Technology, p62
Annual, 1998
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 3510

... RACAL-55
954/846-5151,800/RACAL-55,
Fax: 954/846-3935

Trust Me(TM) **Authentication Server**

The TrustMe(TM) **Authentication Server provides** secure access control for corporate LAN or enterprise network, implementing open system software solutions for...products feature the DES encryption algorithm or an optional proprietary algorithm, and FIPS 140-1 **key** management centers to manage **encryption key distribution** .

SafeDial

The SafeDial(TM) V.34 PCMCIA **provides** portable users with **secure data** communications and remote LAN access over public telephone networks.

Data Security

CRYPTOCard
One First Canadian...916/632-3445
Email: snorton@futurex.com
Web Address: http:/www.futurex.com

SentryLine Data **Security** Products

Sentryline **provides data** and fax **security** using point-to-point authentication and DES. Product includes: SentryModem 336, SertryLink 576, and SentryFax...

...and to authentication of ATM and EFTPOS users.

SafeDial

The SafeDial(TM) V.34 PCMCIA **provides** portable users with **secure data** communications and remote LAN access over public telephone networks.

Trust Me(TM) **Authentication Server**

The TrustMe(TM) **Authentication Server provides** secure access control for corporate LAN or enterprise network, implementing open system software solutions for...

...PCs, Intel, LANs, NEC, Novell Netware, Standalone PCs, WANs, Windows, Windows NT

XONA is a **software** offering which enables **secure delivery** of **data** via the Internet. Its primary component, the XONA Card, is a challenge/response **token programmed** for wire- **transfer** level **security**
.

Film Surveillance Systems

D/B Cameras
1600 E. Valencia Dr., Fullerton, CA
92831; Contact: Tom...

...366-6814
Email: semco@worldnet.att.net
Web Address:
http://www.semshred.com

Model DOG **Security** Waste **Container**

Other Hardware Platform: SEM Shredders

Secure disposal starts with **secure** collection. SEM **containers accept** everything from confidential documents to computer tapes and bound reports into locked, tamper-proof compartments...independent

CUS acts as a "front door lock" to your PBX or centrex lines. CVS **receives** all **access requests** & **verifies** the identity of the individual by their unique voiceprint before transferring them to the protected...